Project 2

Active Directory Environment Setup and Hardening

Rajani Shrestha (155653)

Sadhana Narasimharaj (151584)

Sadhani Lokuge (154551)

Sujitha Govindasamy (154799)

Concordia University of Edmonton

ISSM 505D System and Virtualization Security

Instructor: Benoit Desforges

18th October, 2024

Table of Contents

Executive Summary

This report provides a comprehensive overview of the design, setup, and hardening of an Active Directory (AD) system. The configuration comprised a Domain Controller, a File Server, and a Client Machine, all utilizing Windows Server 2019. We established user and group management, directory permissions, and role-based access control (RBAC). The security posture of the environment was assessed using technologies like PingCastle and CIS Benchmark, followed by the implementation of hardening measures based on best practices. Hardening mesures such as enabling Windows Defender, securing the Recycle bin, disabling SMDv1, refusing LM and NTLM usage and removing users from schema admin roles were applied along with that password policies were also adjusted to enforce stronger security. These actions were taken to mitigate probable vulnerabilities and enhance the overall security of the domain controller.

1. Introduction

The goal of this project was to deploy an Active Directory environment that mirrors enterprise IT infrastructure, focusing on security, access management, and hardening techniques. Active Directory is a critical component in enterprise environments, providing centralized authentication, user management, and policy enforcement.

1.1. Objective

The primary objective of this project is to develop and secure an Active Directory infrastructure that demonstrates proficiency in centralized authentication, user management, and access control. The project specifically aim to:

- Setup a Domain Controller to administer users, groups, and resources.
- Configure a File Server to facilitate shared data access with suitable permissions.
- Implement RBAC to guarantee users access only to the resources pertinent to their responsibilities.
- Utilize security technologies to detect misconfigurations and vulnerabilities.
- Implement hardening techniques to enhance the security posture of the environment.
- Evaluate configurations to verify functionality and security protocols.

1.2. Scope

This project involves setting up and securing an Active Directory (AD) environment with a Domain Controller, File Server, and Client Machine. The tasks include configuring users,

groups, and permissions, implementing role-based access control (RBAC), using security tools for risk evaluation, and applying hardening techniques to improve system security.

2. Environment Setup

The project involved setting up an Active Directory environment with a Domain Controller, File Server, and Client Machine. The Active Directory environment was configured using Windows Server 2019, with the file server and client machine set up as linked clones of the same installation.

2.1. Domain Controller Setup

Domain Controller is the server responsible for managing the network and access control of the user and computer with the domain (*What Is a Domain Controller? - IT Glossary*, n.d.). Following steps are followed to setup of the domain controller in this project.

2.1.1. Installing Domain Controller

The Windows Server 2019 computer was set up as a Domain Controller to lay the groundwork for the Active Directory (AD) infrastructure. This required promoting the server to administer the domain 505Group4DC.local and installing the "Active Directory Domain Services" (AD DS) role. The following steps indicate the Installation of Domain Controller:

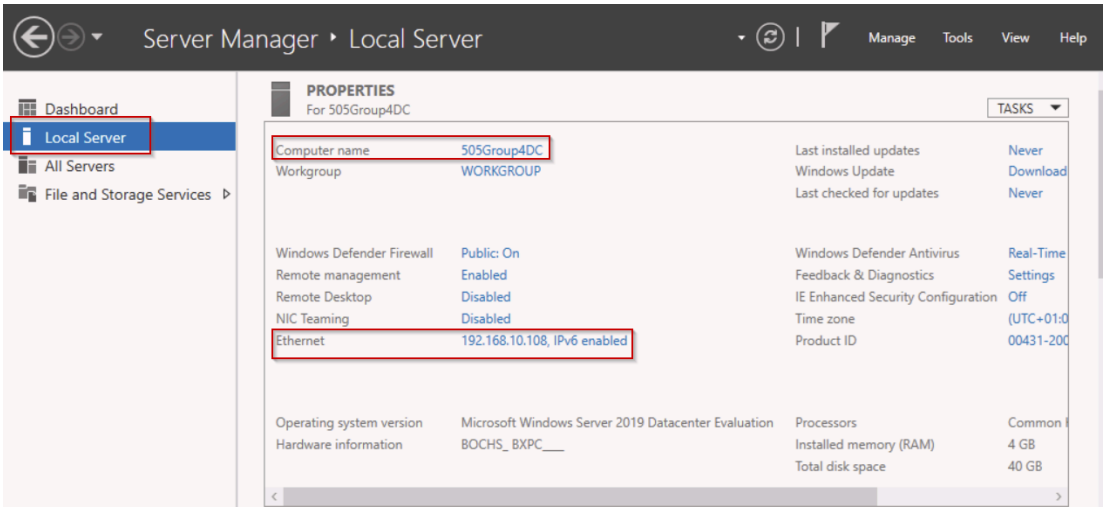


Figure 1: Initial setup for active directory

- The Windows Server 2019 machine was designated as 505Group4DC under the workgroup - WORKGROUP, in order to provide effective domain identification.

- For stable and reliable network connectivity, a static IP address - 192.168.10.108 was set up.

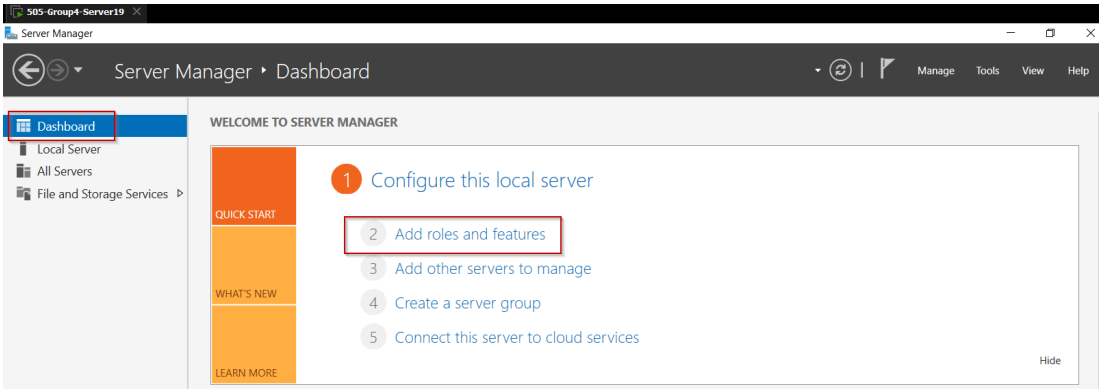


Figure 2: Adding roles and features

- After launching the Server Manager, "Add Roles and Features" was chosen.
- Decided to move forward with a feature-based or role-based installation.

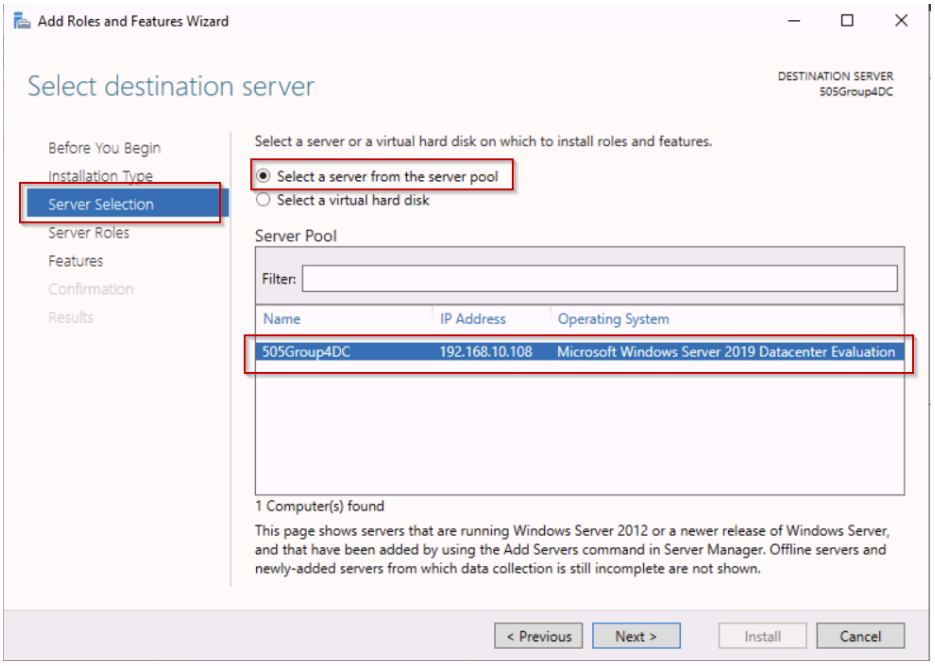


Figure 3: Selection of DC server from server pool

- For the installation of necessary roles, the server- *505Group4DC* was chosen as the target server from the server pool.

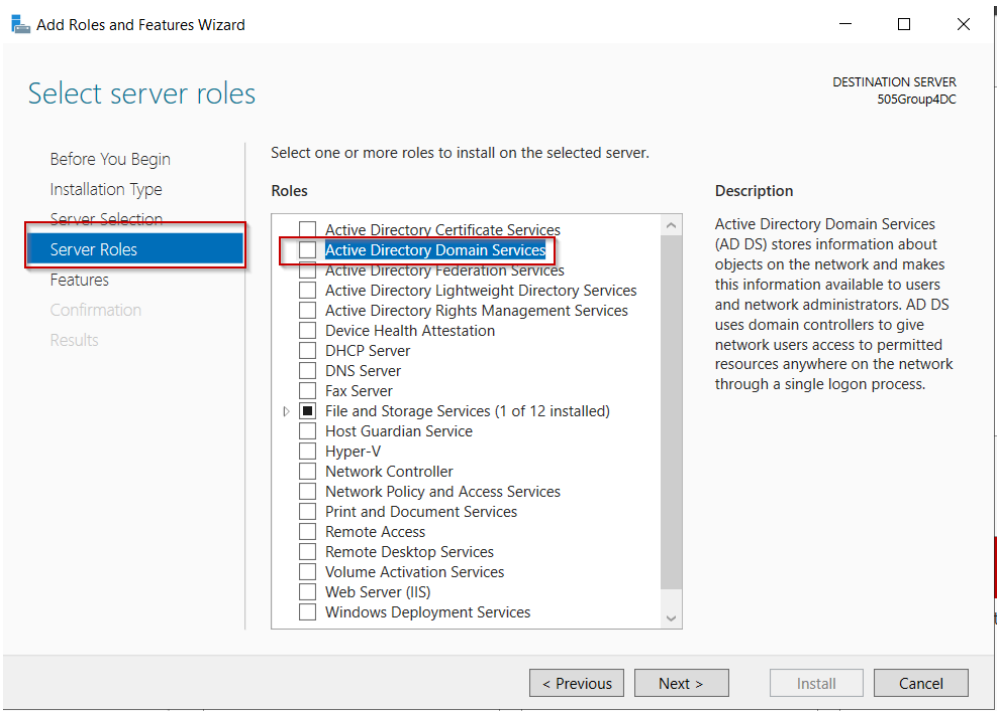


Figure 4: Adding ADDS to server roles

- Out of the server roles listed, the Active Directory Domain Services (AD DS) role was chosen.
- The installation process included the addition of necessary management tools.

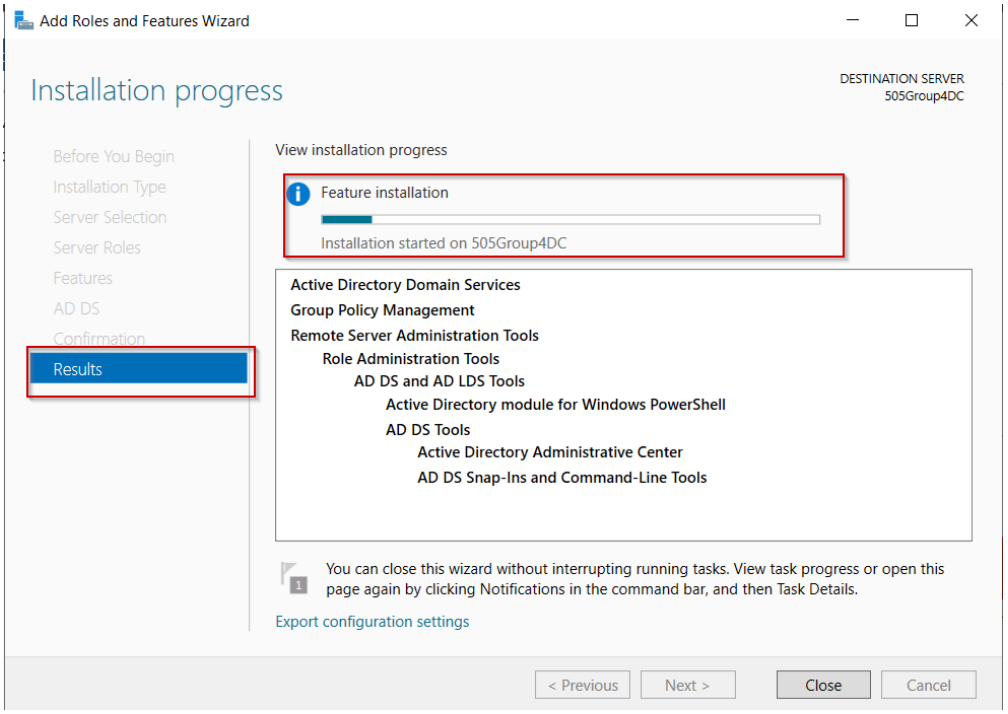


Figure 5: Installation of ADDS with selected tools

- The installation procedure was started when the AD DS and other tools had been chosen.

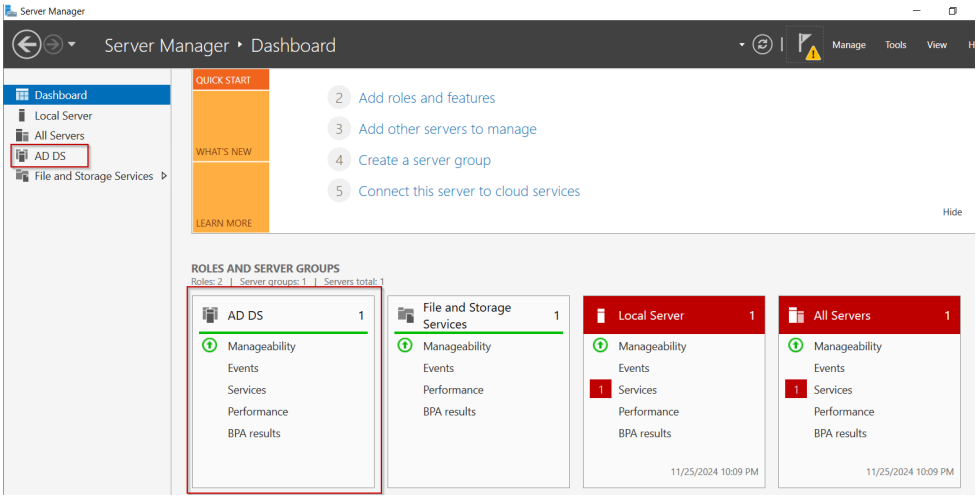


Figure 6: ADDS availability in the dashboard

- The Installation was confirmed to be successful when the AD DS role was shown in the Server Manager Dashboard.

2.1.2. Promoting to Domain Controller

After the successful Installation of the Active Directory Domain Services (AD DS) role, the process of promoting it to a Domain Controller (DC) was initiated. This procedure turns the server into a domain-wide central location for resource, device, and user management and authentication. By this the AD DS server - *505Group4DC*, will be able to manage essential directory functions, including access control, policy enforcement, and user authentication, which are the foundation of an Active Directory (AD) infrastructure. The database and log paths are also configured in this stage. When finished, the server is prepared to manage directory and authentication services as a fully functional Domain Controller. The following steps indicate the Promotion of the Server to a Domain Controller:

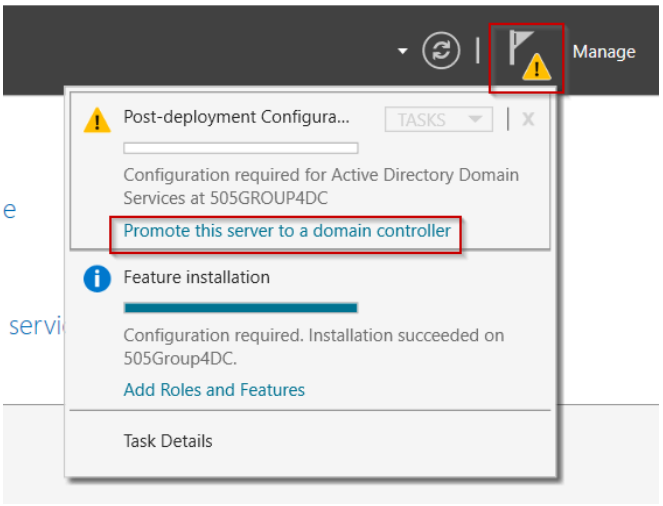


Figure 7: Promoting the 505Group4DC Server to Domain Controller

- The Promotion Process was initiated by accessing the Server Manager Dashboard and choosing the "Promote this server to a domain controller" option.

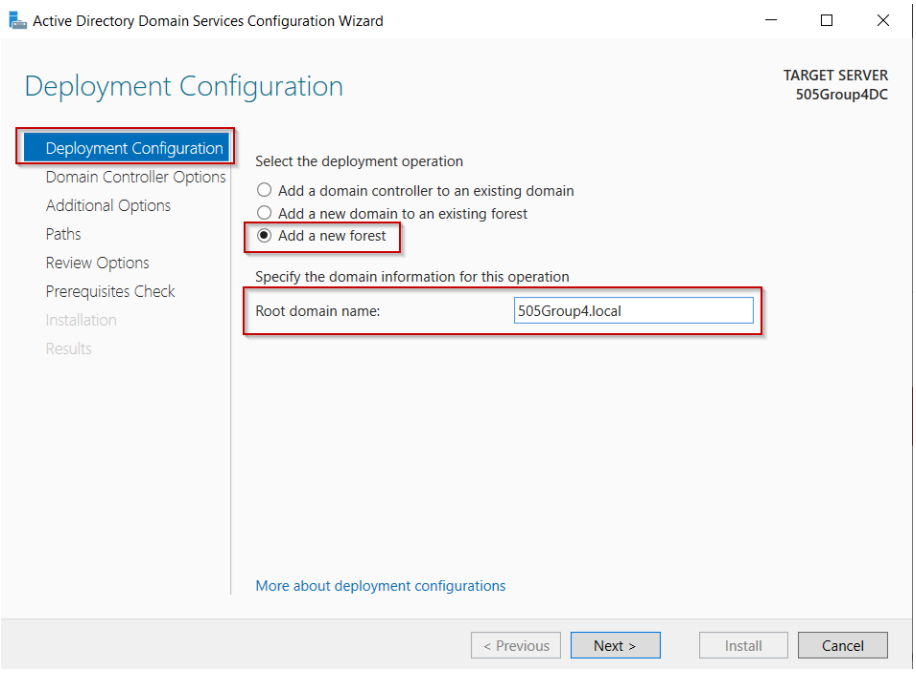


Figure 8: Addition of new forest with domain name - 505Group4.local

- The idea of adding a new forest, stated with the specification of the domain name - *505Group4.local* in the deployment configuration.
- The domain's NetBIOS name, *505Group4*, was produced automatically.

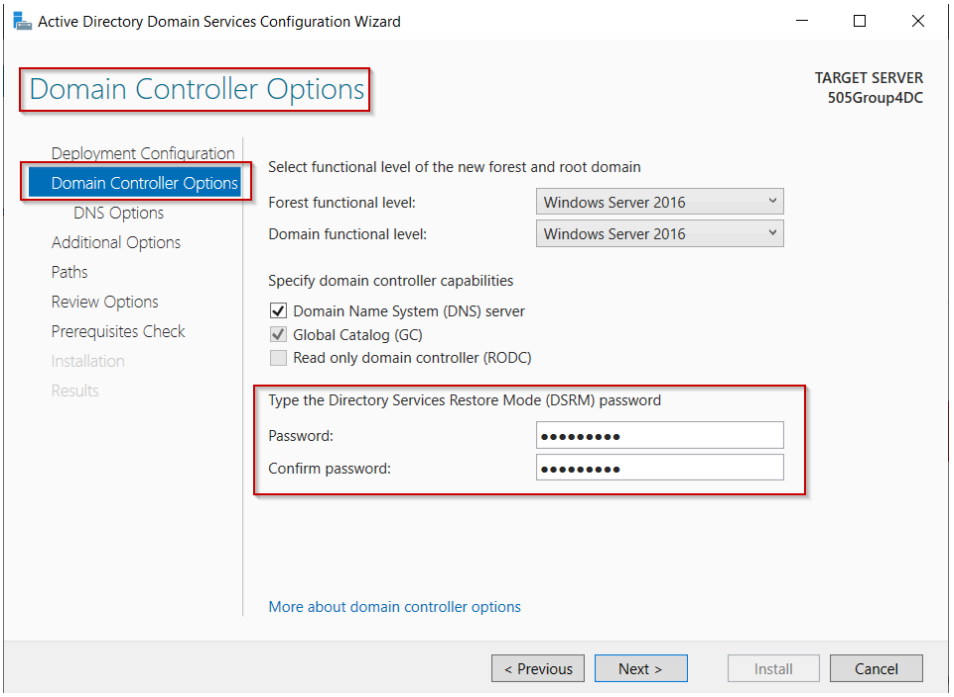


Figure 9: Setting the DSRM password

- The next step was to select the Forest and Domain levels, which was set to *Windows Server 2016* and the DC capabilities included DNS server and global catalog(GC).
- To facilitate domain maintenance and recovery, a strong DSRM password was established.

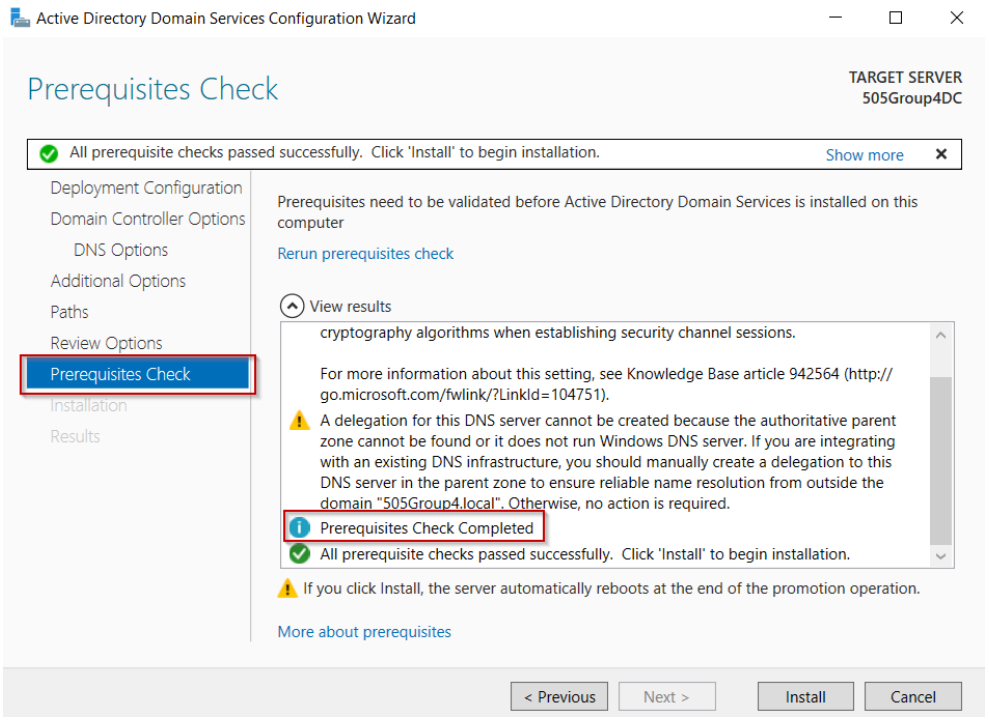


Figure 10: Completion of Prerequisites check

- To make sure all requirements for the server promotion were satisfied, the installer performed a Prerequisites Check, which was completed successfully.

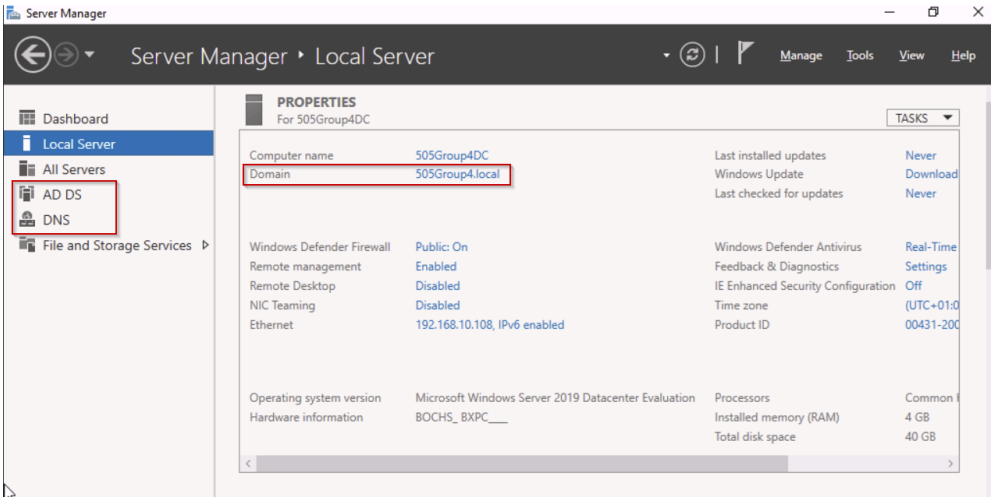


Figure 11: Successfully promoting the server to DC

- To implement the modifications, the server was rebooted after being successfully promoted to a Domain Controller.

2.1.3. Organizational Unit (OU)

When the Domain Controller was being built up, the Users and Computers containers were automatically created. Custom OUs were not necessary because user and machine accounts were managed and organized using these default OUs.

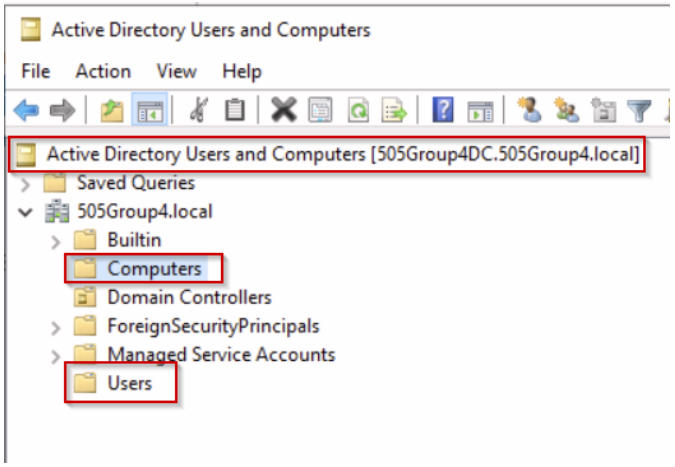


Figure 12: Creation of DC users

2.1.4. Creating Group in AD

Since the default Organizational Units (OUs) were used, the appropriate location for creating groups was the 'Users' container in Active Directory. Since the default OUs have been used in the previous step instead of any customization, the groups have to be created under the “Users” container in AD. Two groups, Test1 and Test2, were made inside this container in order to efficiently handle rights and arrange users. The following steps indicate the Creation of Groups in a Domain Controller:

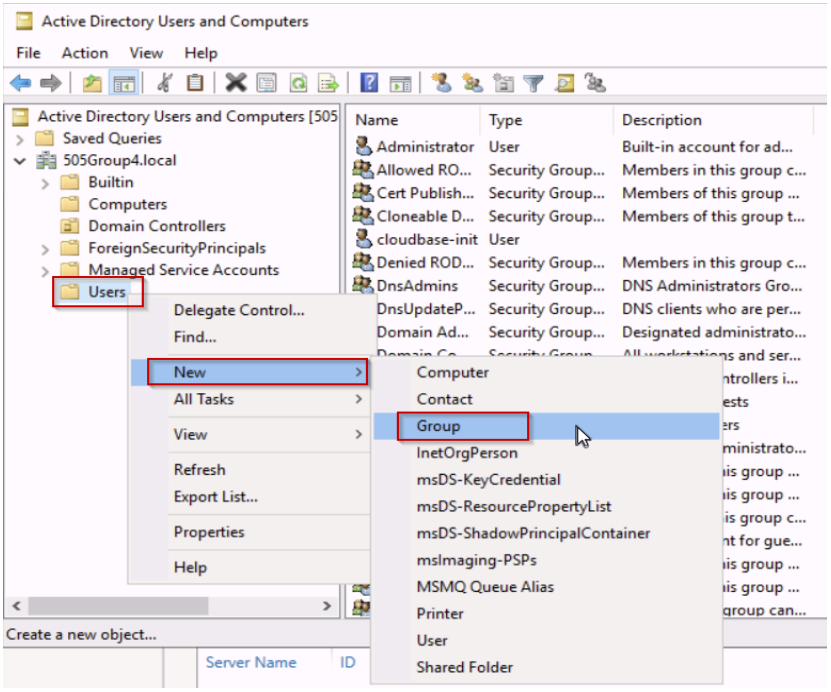


Figure 13: Creation of Groups in DC

- The Active Directory Users and Computers console was accessed and navigated to the Users container.
- After choosing the 'Users' container, creation of two new groups, Test1 and Test2 were initiated .

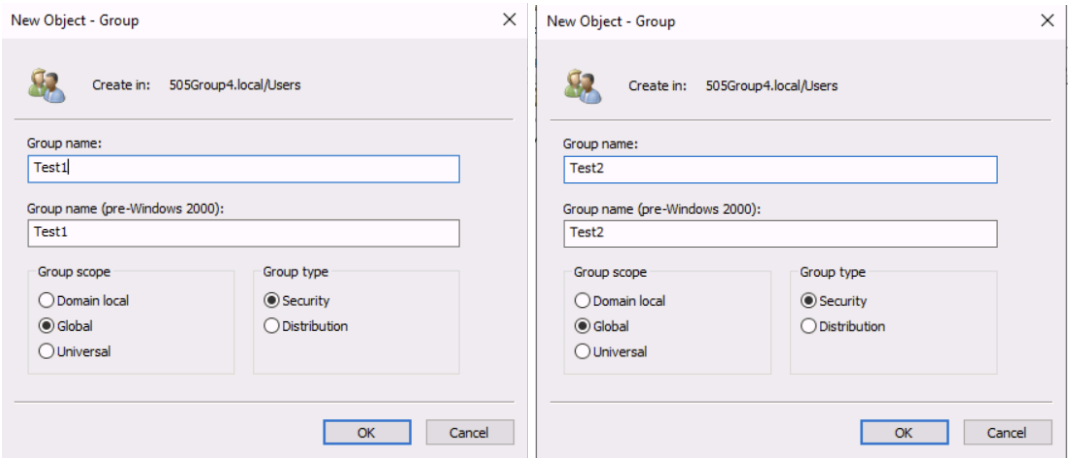


Figure 14: Creation of Group - Test1 & Test2 and assigning scope

- Assigned Group names to Test1 and Test2 and selected the group type to Security Group.
- During formation, the groups scope (e.g., Global or Domain Local) was defined as Global for both Test1 & Test2.

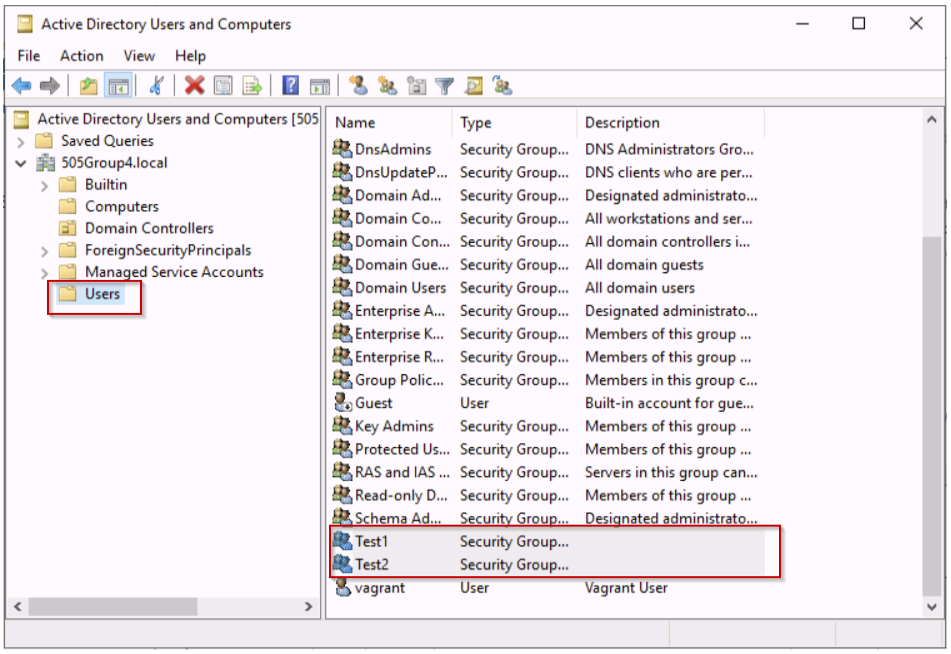


Figure 15: Successful creation of the group under Users

- The successful formation of the groups Test1 and Test2 was indicated by their appearance under the 'Users' container with type security group .

2.1.5. Creating User Accounts in AD

The user account April was created in Active Directory under the User container of default Organizational Unit, as shown in the screenshot below. Following the creation of

April, four additional user accounts ; May, June, July, and August, were created in the same manner. These accounts were added to the domain, ensuring they meet the required password policies. The following steps demonstrate this user creation:

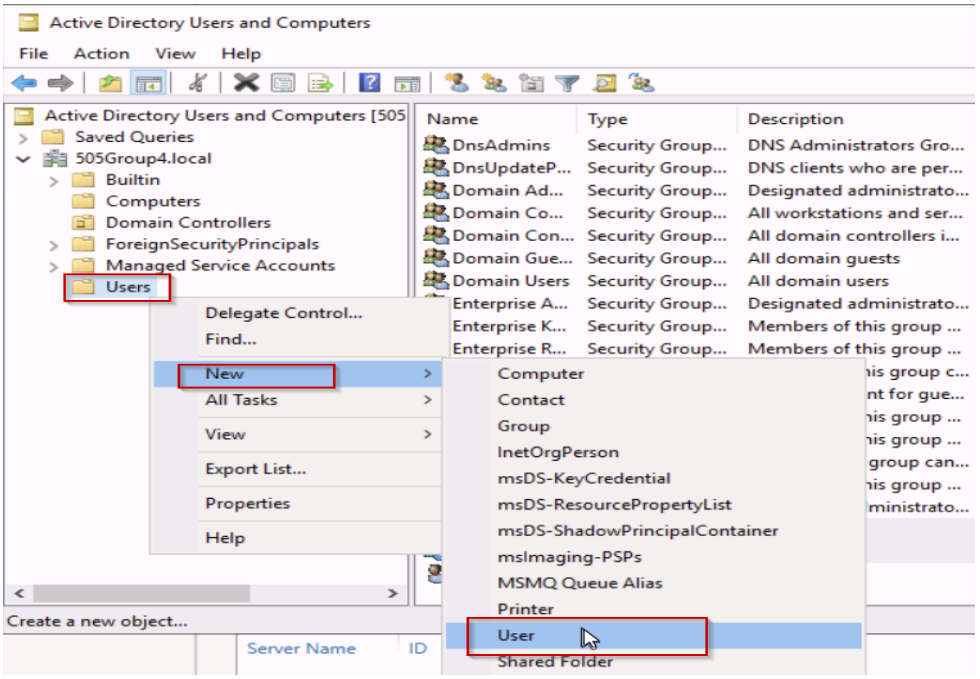


Figure 16: Creation of new user accounts under Users

- For the creation of new users, the same path used for group creation was followed. The Active Directory Users and Computers console was accessed and navigated to the Users container.
- After choosing the 'Users' container, creation of new users, April, Mayb, June, July and August were initiated .
- For every user, a designated username and a secure password was assigned.

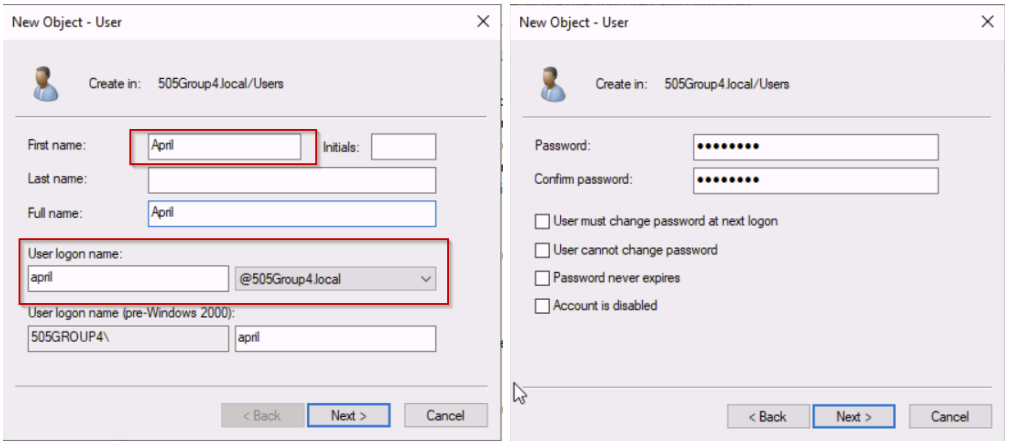


Figure 17: Creation of User - April and assignation of password

- Each user's password was configured, and adherence to the domain's password restrictions (such as minimum length and complexity) was guaranteed.

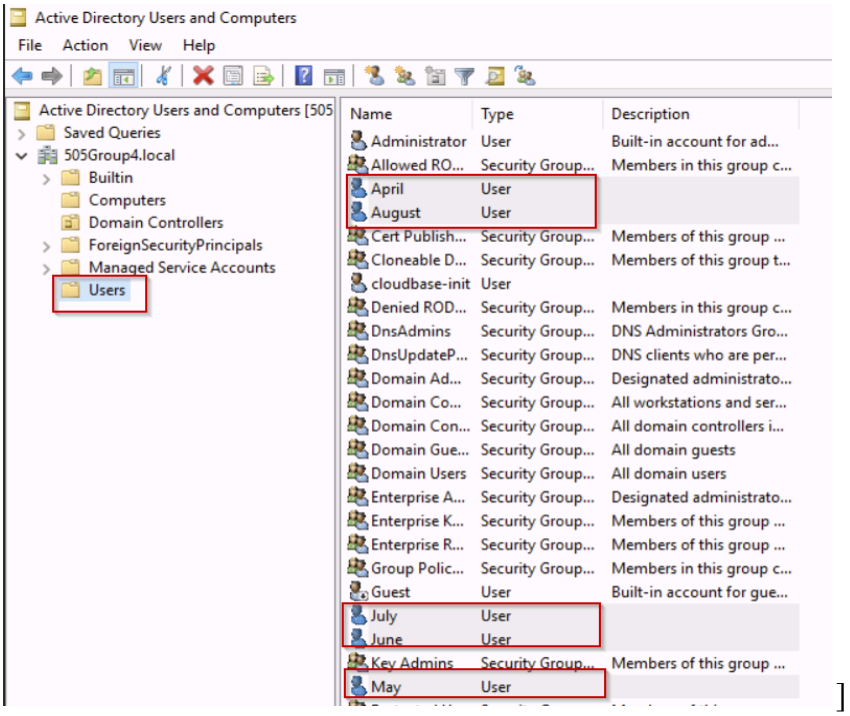


Figure 18: Successful creation of the above users under Users

- The successful creation of the newly formed users was confirmed when they appeared in Active Directory under the 'Users' container.

2.1.6. Adding Users to created group

This step demonstrates how users are assigned to groups for effective role-based access control. This approach simplifies permission assignment by associating specific roles and access levels with groups rather than individual users.

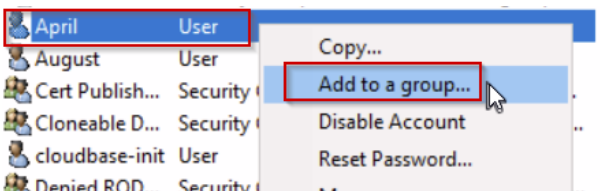


Figure 19: Adding the created users to a group

- selected an user and brought up their Properties pane (for example, April).
- Then, this user is added to a group by navigating to the Member Of tab.

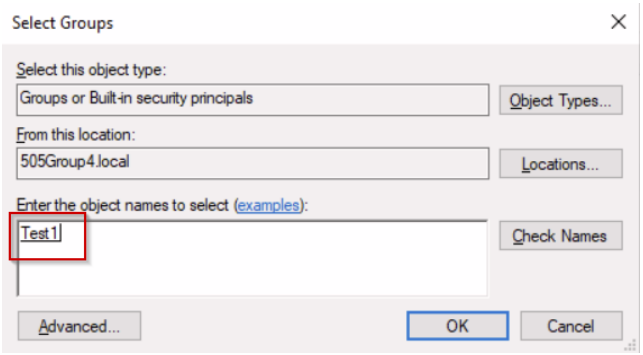


Figure 20: Selecting the group to add users

- From the list of available groups, selected the relevant groups created in the previous step (such as Test1 or Test2) and the user was added to that group.

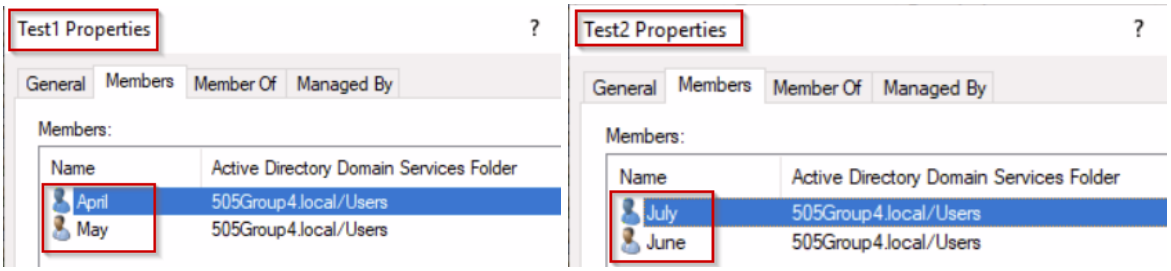


Figure 21: Adding users to the Test1 and Test2 groups

- Verified that the user had been added to the chosen group.
- Confirmed that the additions of April and May to Tests1, July and June to Test2 respectively, were successful.

2.2. File Server Setup

File Server was configured and setup to manage the access control of user that was created in domain controller (Wright, n.d.) which can be shown in the steps below:

2.2.1. Joining File Server to Domain Controller

This picture shows how the file server is connected to the Active Directory-controlled domain. Entering the domain name and administrator credentials in the "System Properties" box joins the server to the domain. If this stage is completed successfully, the file server is included in the network infrastructure that is centrally administered.

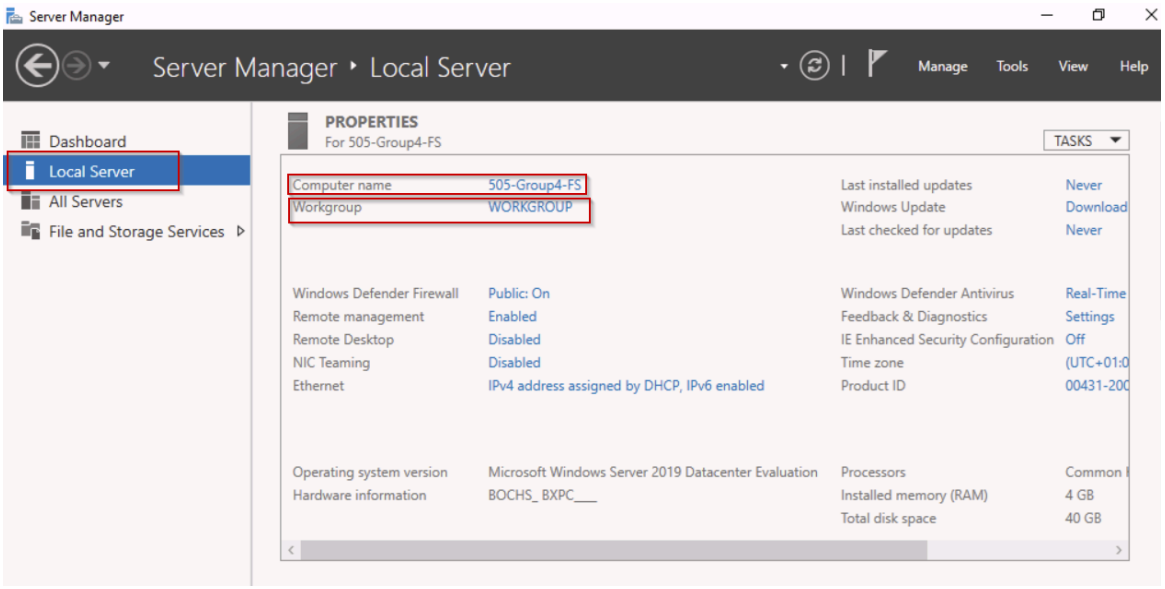


Figure 22: Initial setup for file server

In the initial setup of the file server, the workgroup is set to "Workgroup," which will be changed to a domain controller at the end of the setup. The computer name is configured as "505-Group-FS" to identify and manage the machine as the file server.

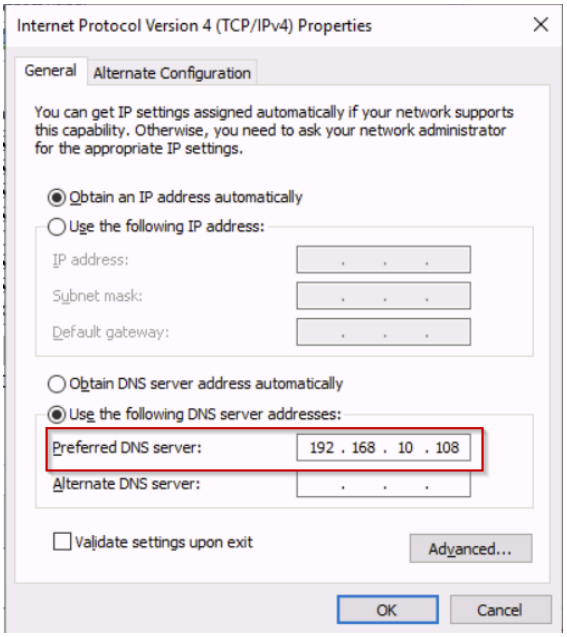


Figure 23: Adding preferred DNS to dc ip

First, to join the file server to the domain controller, we need to modify the network settings on the file server. Specifically, the "Preferred DNS" on the file server should be set to the Domain Controller's IP address, which in our case is "192.168.10.108." This

configuration ensures that the file server can properly locate and communicate with the Active Directory services hosted on the domain controller.

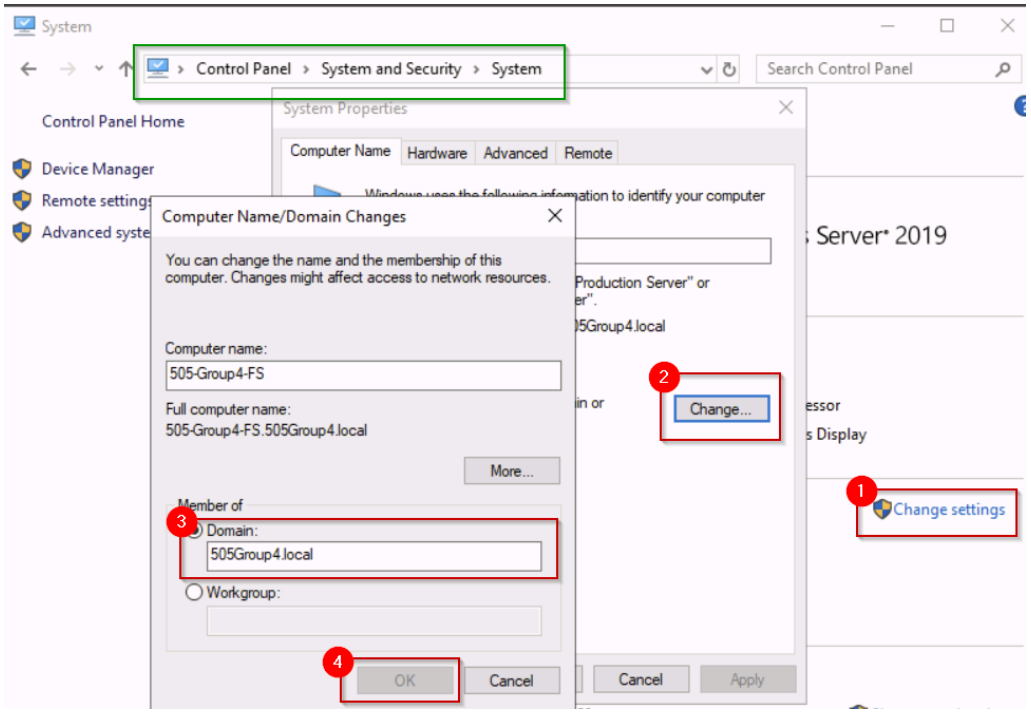


Figure 24: Steps to add file server to domain controller

In the figure above, we can see the steps to add the file server to the domain controller. To do this, we need to navigate to **Control Panel > System and Security > System**, then click on **Change settings** and select **Change** next to the computer name. Here, we will enter the domain name that we configured for the domain controller, which is **505Group4.local**. After entering the domain name, an authentication screen will appear, where we authenticate using the domain user credentials. This process leads to the successful joining of the file server to the domain controller.

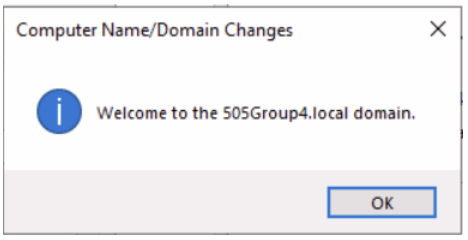


Figure 25: Confirmation Screen of adding fs to dc

In the figure below, we can see that the workgroup has been changed to **Domain** with **505Group4.local**, confirming that the file server is now the part of the domain controller.

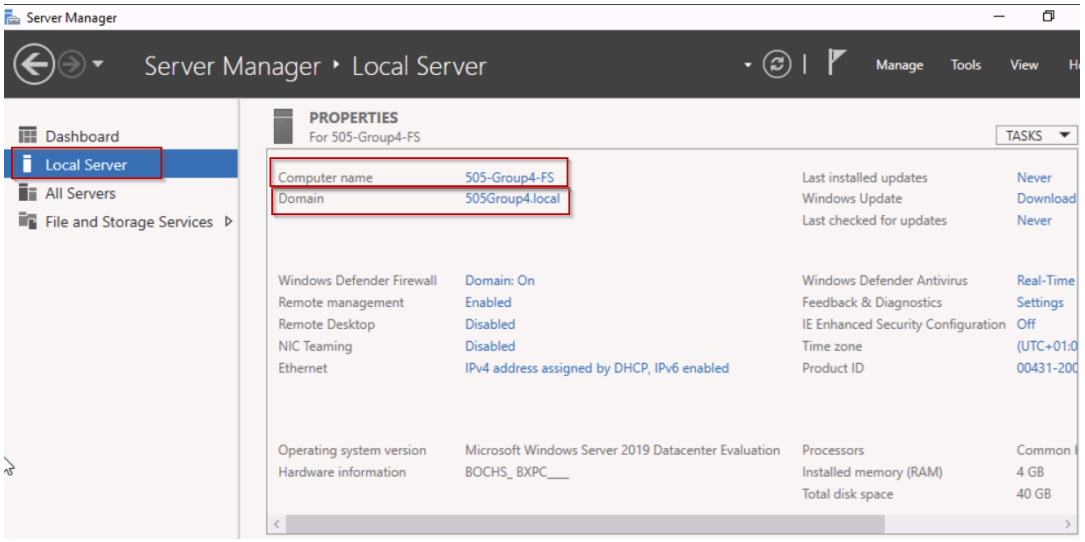


Figure 26: File server added to domain controller

2.2.2. Adding "File Server" Role

The addition of the "File Server" role via the Server Manager is shown in another figure. With this function, the server can serve as the domain's central repository for managing and storing shared files. Effective data management and access control are made possible by the setup, which provides the directory structure needed for the project.

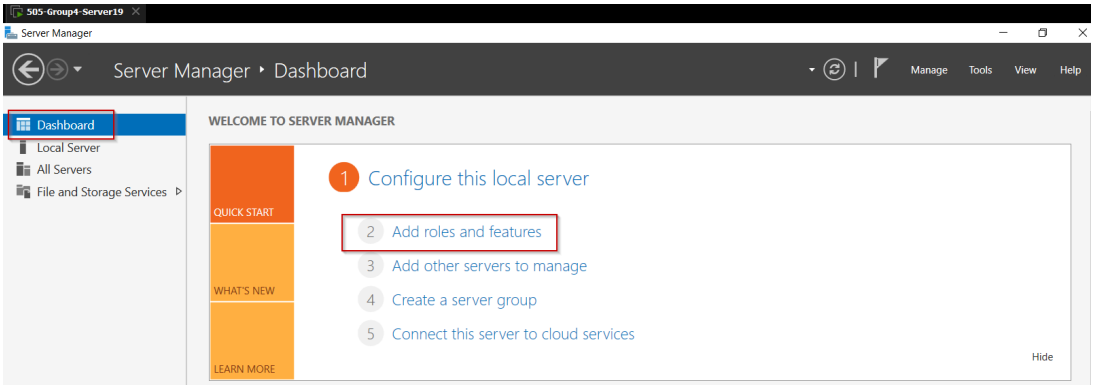


Figure 27: Adding roles and features for File Server

To add the "File Server" role in server, we clicked "Add roles and Features" like we have done while adding active directory service.

Then the server pool was selected which is the IP of file server ***"192.168.10.106"*** as shown in figure below:

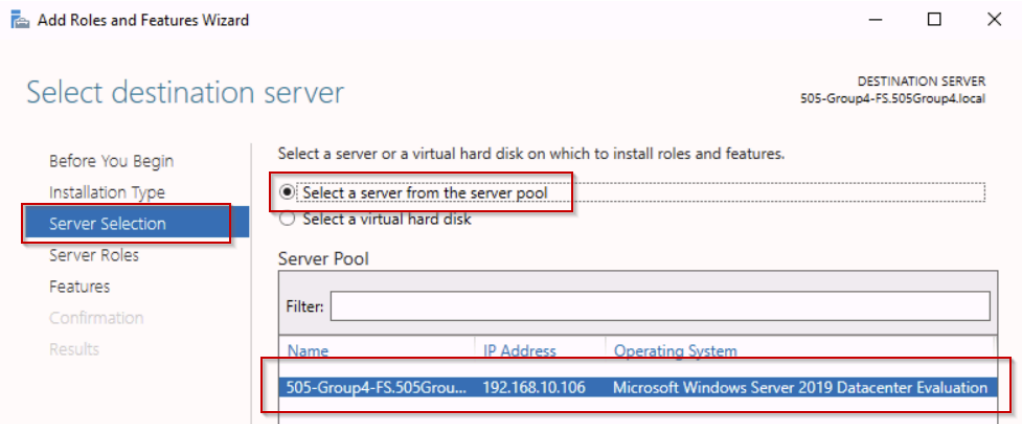


Figure 28: Selection of 505-Group4-FS from server pool

After selecting the server where we want to install the file server, the next step is to choose the roles to be installed. In this case, we select the **"File Server"** role, which can be found under the **File and Storage Services** section. This role enables the server to function as a file server, allowing it to store and manage files shared across the network.

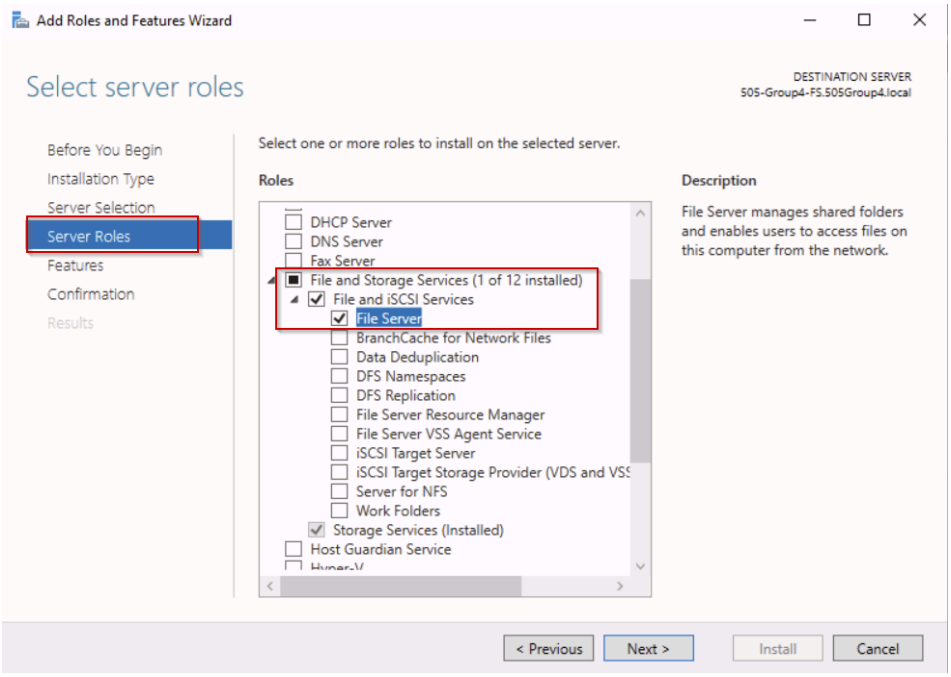


Figure 29: Assigning File Server role to 505-Group4-FS

The figure below shows the feature installation progress.

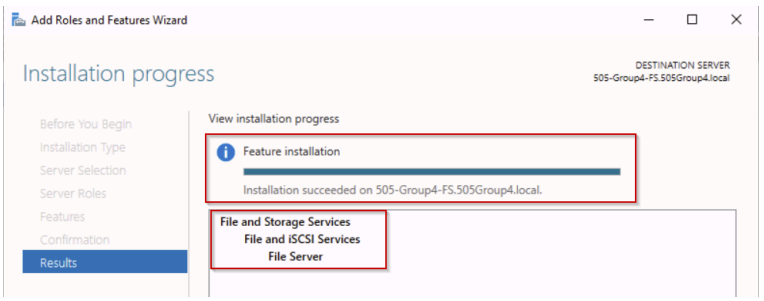


Figure 30: Installation of FS with selected services

Verification of the file server being installed is shown in the figure below.

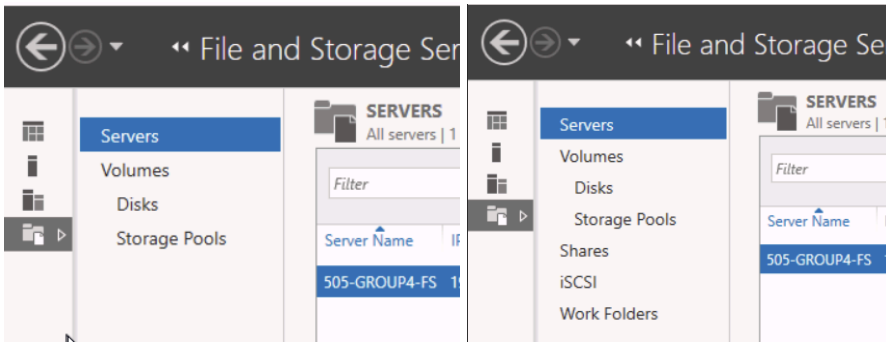


Figure 31: File Server available under All Servers

2.2.3. Disabling automatic Updates

Disabling automatic updates helps maintain control over when and how the system is updated, preventing important functions from being interrupted. By turning off automatic updates, the administrator can manually review and schedule updates at a time that causes minimal disruption. To disable automatic updates on the file server, search Local Policy Editor on the system. Then navigate to Computer Configuration> Administrative Templates> Windows Components> Windows Update> Configure Automatic Updates as shown in the figure.

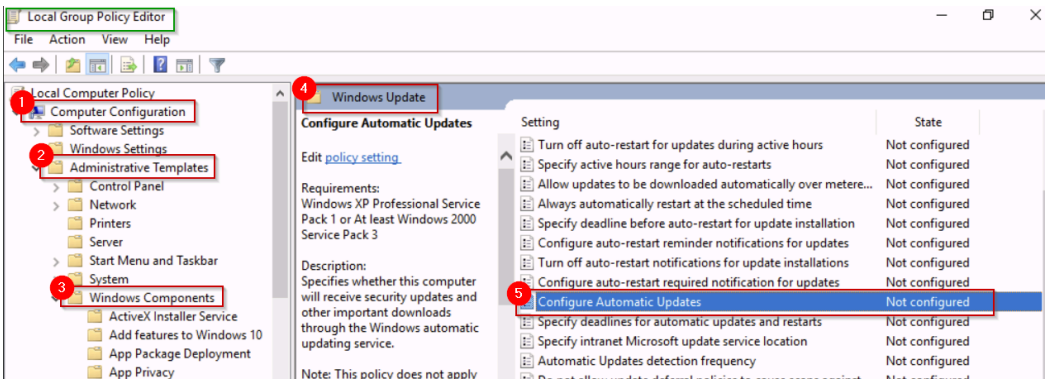


Figure 32: Accessing configuration of automatic updates

In the configuration window, set it to "Disabled" as shown in the figure below. This will successfully disable automatic updates.

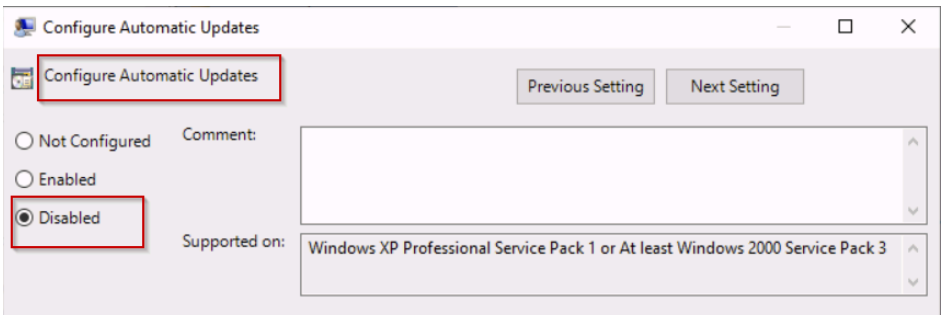


Figure 33: Disabling configuration of automatic updates

2.2.4. Creating a Directory

The directory structure was put in place to effectively manage and arrange data. At the root of the C: drive, a primary folder called TestData was established. Three subcategories were added to this folder: Users, Jobs, and Accounts.

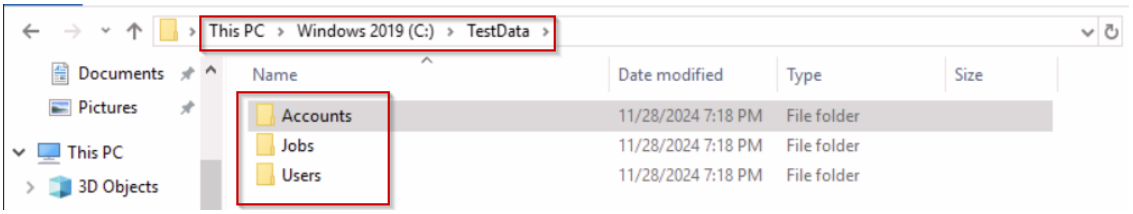


Figure 34: Creation of the TestData directory

2.3. Client Machine Setup

Similar steps were taken to connect the client computer to the domain controller as they were for the file server.

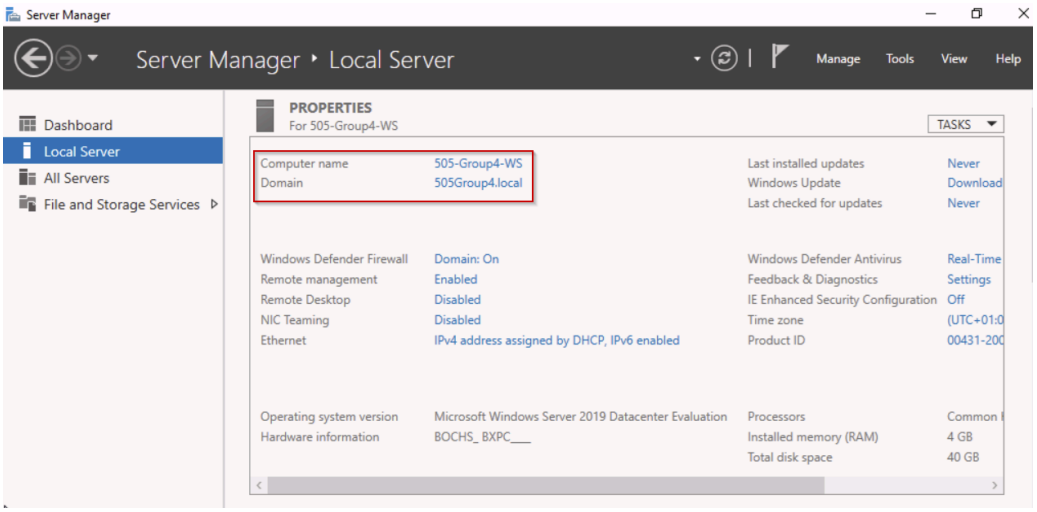


Figure 35: Client Machine Joined to domain controller

3. Permission Setup

Various permissions were configured for each folder created on the file server to understand and implement access control effectively.

3.1. Granting all user access to “Users”

The first permission to be set is granting all users access to the "Users" folder. To achieve this, first we need to add all users to the folder before applying the permission. The users April, May, June, July, and August can be added to the folder permissions by clicking the Add button in the “Permissions for Users” section, as highlighted by the green box in the figure before setting permissions to them. By clicking Add, these users can be authenticated and selected from the domain controller, allowing them to be included in the folder's permission settings.

The figure below shows the step for granting all user access to the folder “Users”. To achieve this navigate to Users > Properties> Security>Edit, Select the user to which we want to set the permissions, in our case it is April, May, June, July and August. Set the permissions to “Full Control” giving full access to all the uses and apply the setting.

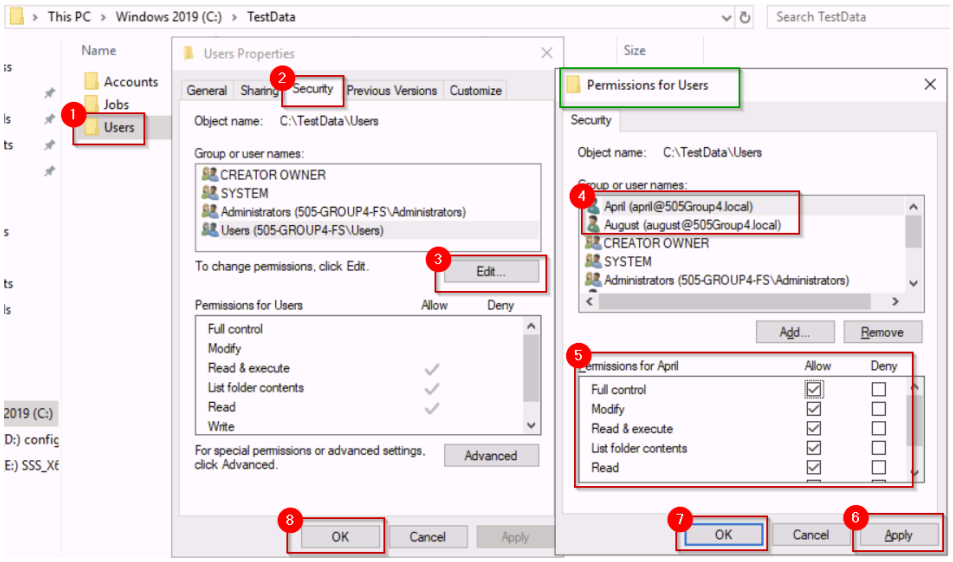


Figure 36: Granting permission to all users to access Users

3.2. Giving “Test1” access to modify “Jobs”

We also set the "Modify" permissions for the "Jobs" folder for the Test1 group, following the same steps as we did for the previous configuration. With this permission users on Test1 group - April and May should be allowed to modify the content within the Jobs folder.

Steps for adding modify permissions include: navigating to Jobs > Properties> Security>Edit, Select the user or group to whom we want to set the permissions, in our case isTest1 (April and May). Set the permissions to “Modify” giving access to add, edit and delete to the user and apply the setting. The step can be seen in the figure below.

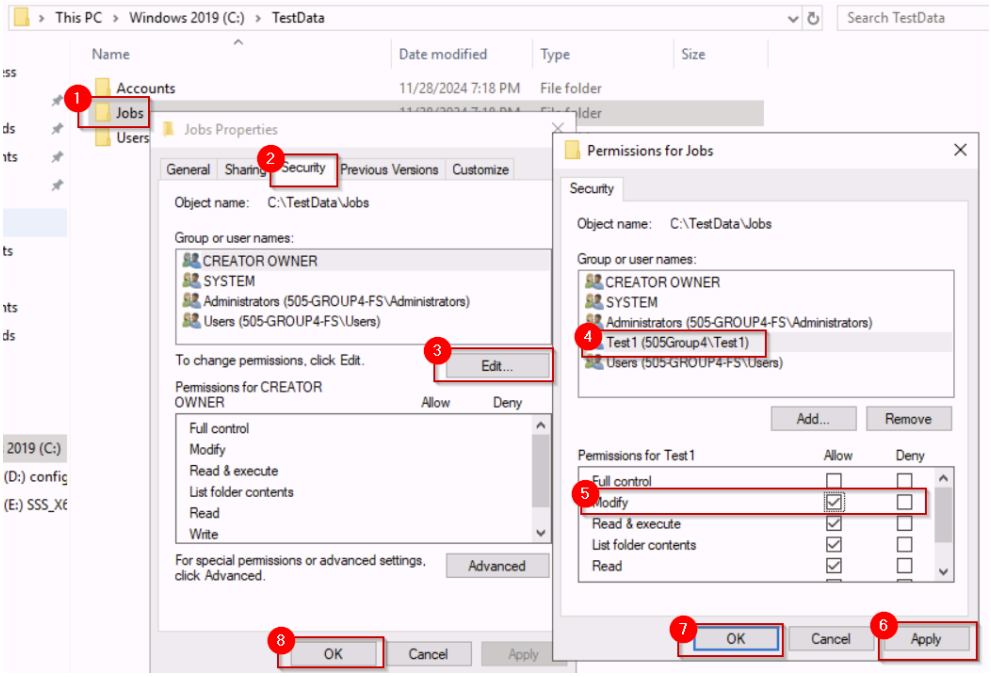


Figure 37: Granting permission to user - Test1 to modify

3.3. Giving “Test2” access to read and write in “Accounts”

"Read and Write" permissions was set to "Accounts" folder for the Tes21 group, following the same steps as we did for the previous configuration. With this permission users on Test2 group - June and July should be allowed to only read and write the content within the Accounts folder. However, the users will be restricted for performing any other task such as editing and deleting.

Step for adding read and write permissions include: navigating to Jobs > Properties> Security>Edit, Select the user or group to whom we want to set the permissions, in our case isTest2 (June and July). Set the permissions to “Read and Write” giving access just to read and write on the folder to user and apply the setting which is shown in the figure below.

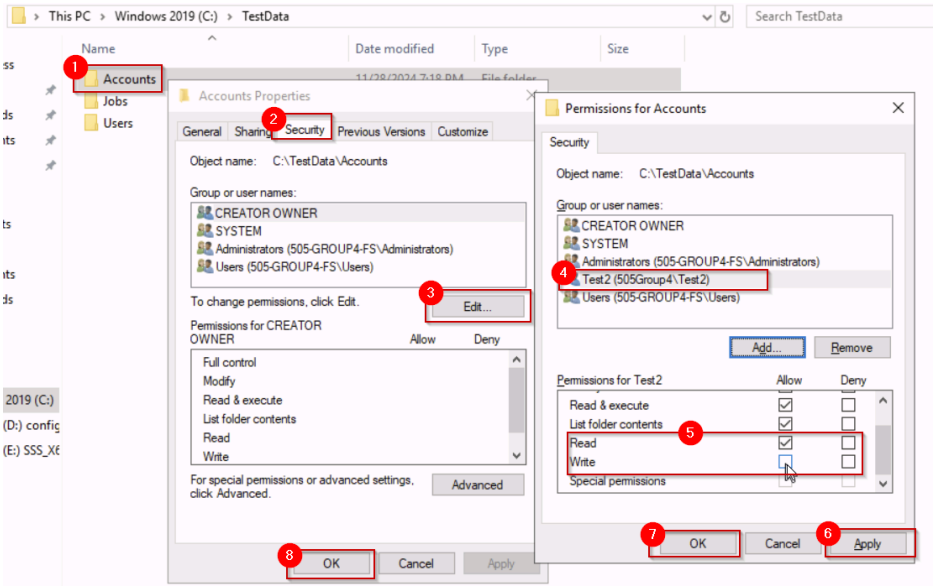


Figure 38: Granting permission to user - Test2 to read & write

3.4. Giving user "August" permission to read "Jobs"

For user August, read-only permission is granted, following the same steps as we did for the previous configuration. With this permission user August is just allowed to read the file and is restricted to perform any other task.

Step for adding read permission include: navigating to Jobs > Properties> Security>Edit, Select the user or group to whom we want to set the permissions, in our case is August. Set the permissions to "read" only giving access to read to user and apply the setting as shown in the figure below.

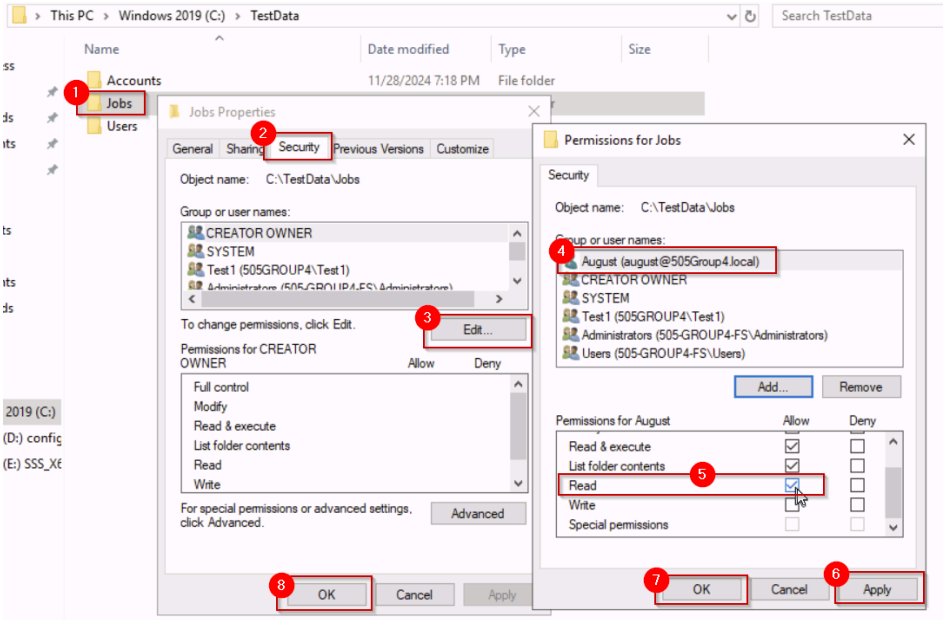


Figure 39: Granting permission to user - August to read

4. Role Based Access Control Exploration

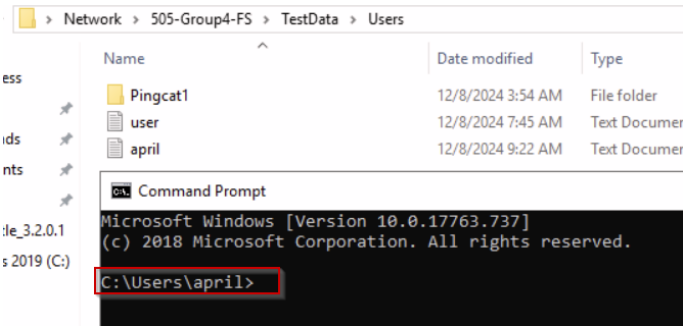
Role-Based Access Control (RBAC) enables users to perform tasks based on the roles assigned to them (David F. Ferraiolo and D. Richard Kuhn, n.d.). When a user is assigned to a specific group, their actions are limited to the permissions associated with that role, restricting access to unauthorized tasks.

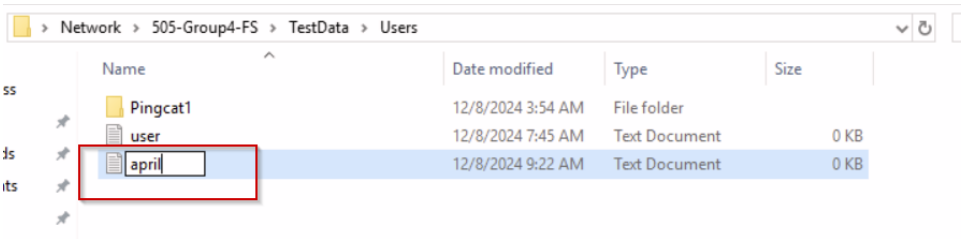
4.1. Login to Client Machine and testing folder access from Client Accounts

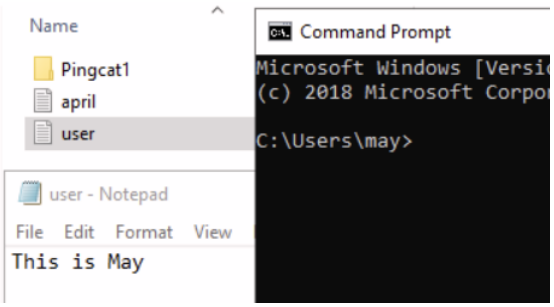
First of all, to test the folder access permissions set in the previous step, the client machine was accessed using the authentication credentials of each user (April, May, June, July, August).

- **Testing all user access to User Folder**

All users were granted full access to the Users folder. This access was tested and successfully verified, as demonstrated in the figure below.







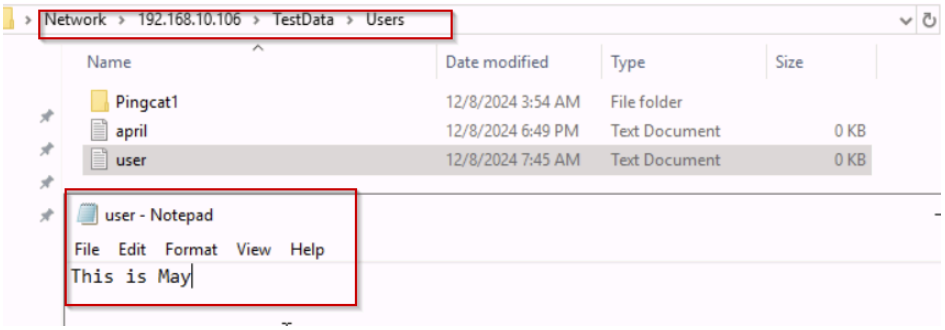


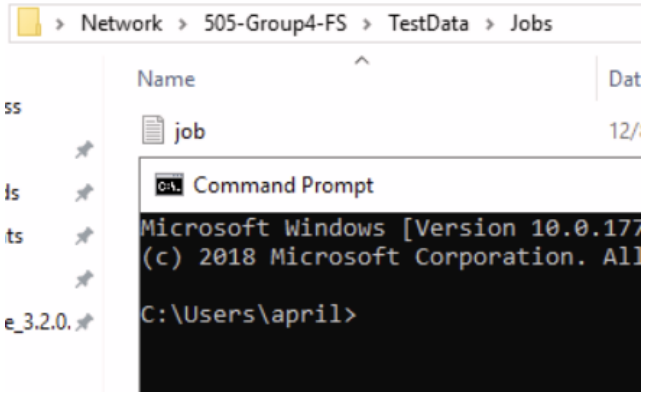
Figure 40: Testing all users access

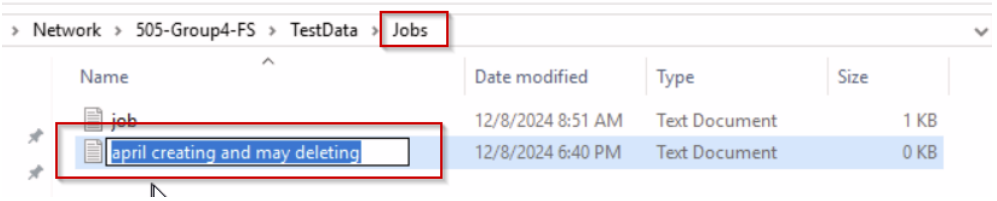
- **Testing Test1 Access to modify Jobs**

  Users in Test1 - ***April and May***.

  The figure below demonstrates that both users, April and May, in Test1 group have permission to modify(add, update and delete) the content in the Jobs folder but are denied access to perform any actions in the Accounts folder.

  Here, as user April, a file was successfully created in the "Jobs" folder. However, attempting the same action in the "Accounts" folder showed a "Folder Access Denied" message, as shown in the figure below.





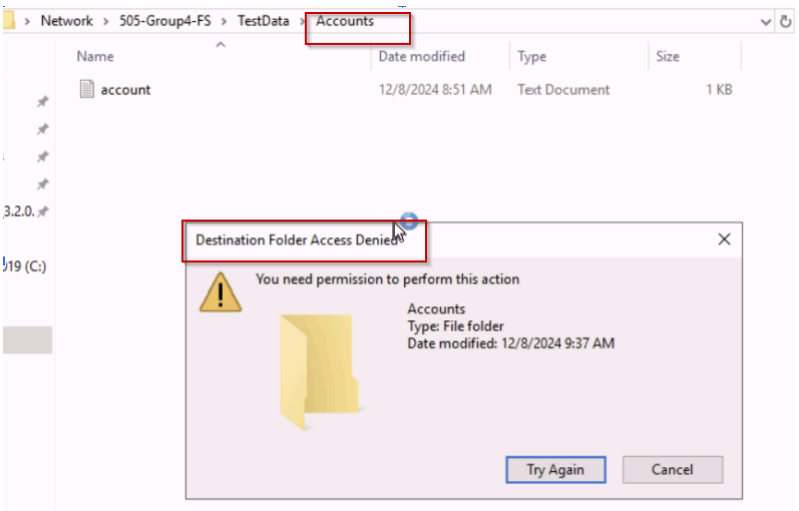
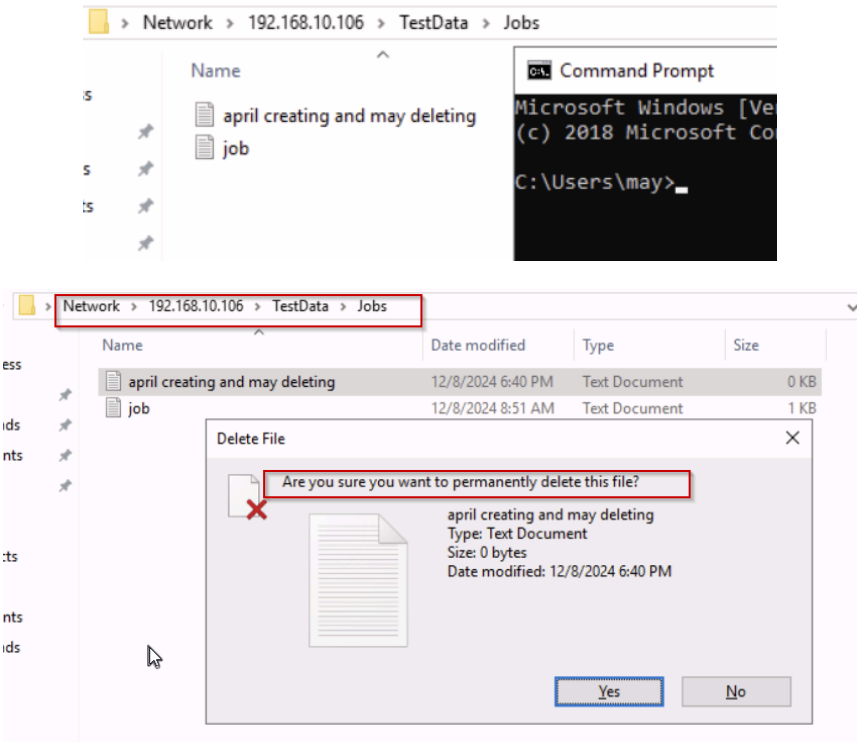


Figure 41: Testing Test1 user access

As shown in the figure below, while logged in as user May, a file was successfully deleted in the "Jobs" folder. However, attempting the same action in the "Accounts" folder resulted in a "Need Permission" message.



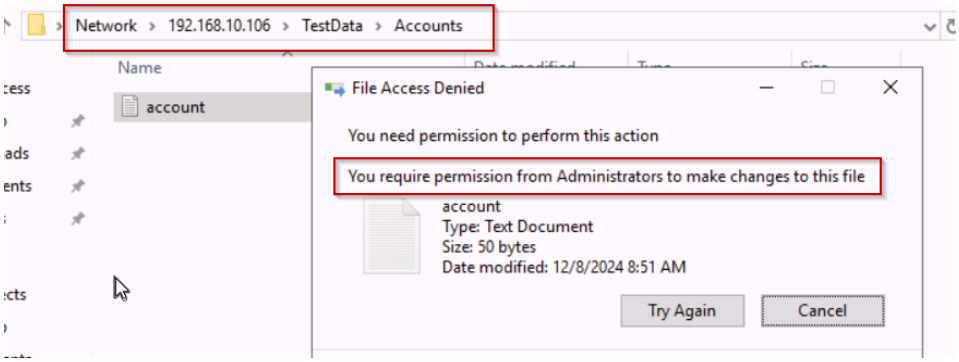
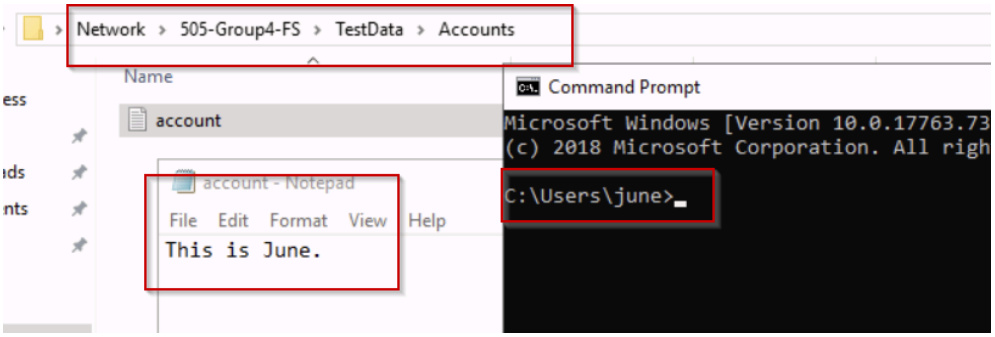


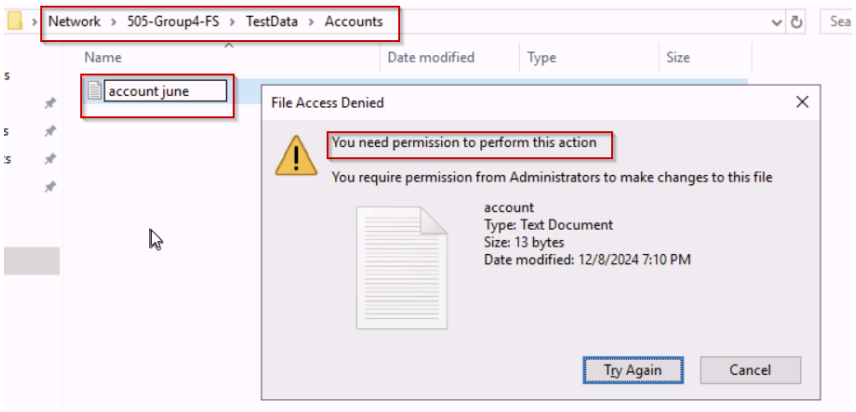
Figure 42: Testing Test1 user access

- **Testing Test2 to Read and Write in Accounts**

  Users in Test2 - ***June and July***

  As shown in the figure below, both users, June and July, from the Test2 group can only read and write in the "Accounts" folder. They are restricted from performing any other actions, including making changes to the "Jobs" folder.





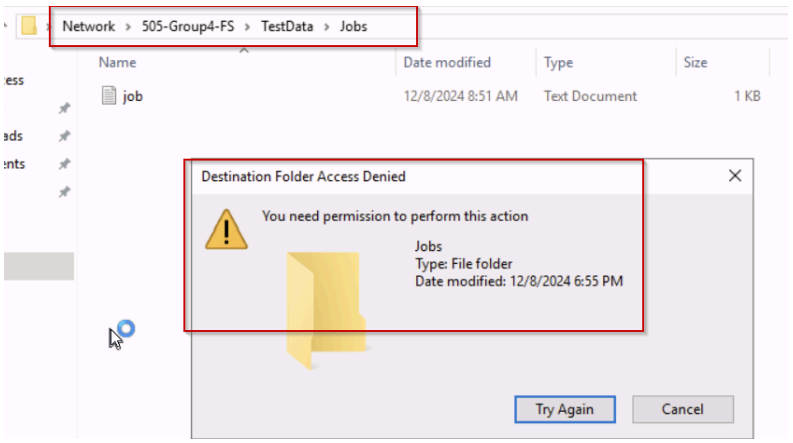
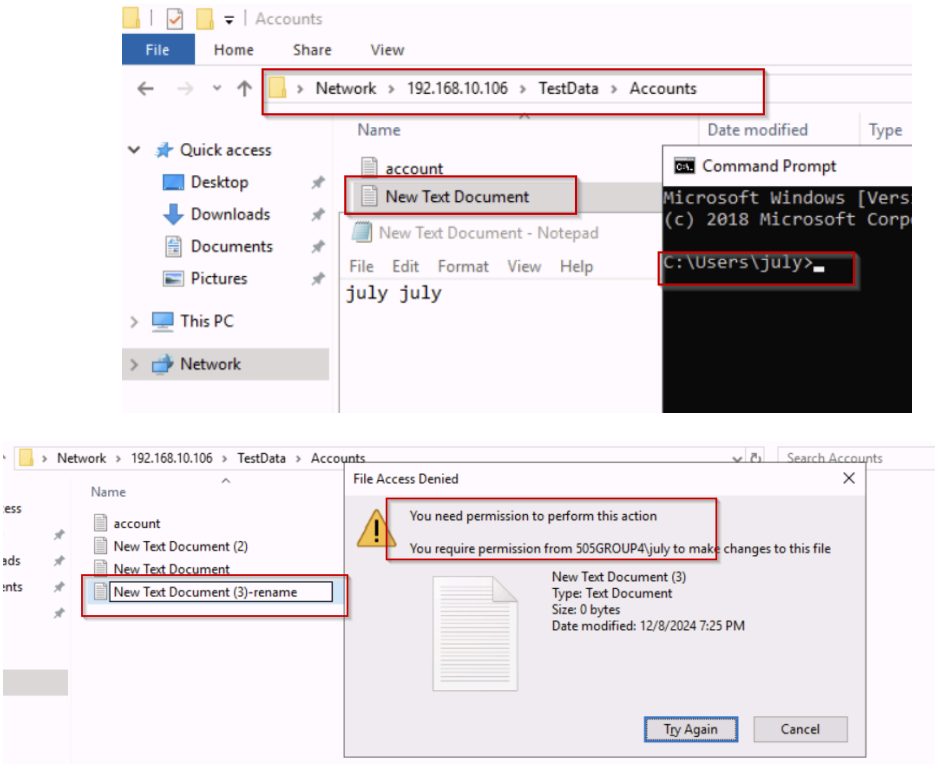


Figure 43: Testing Test1 user access

As user July, we attempted to create a file in the "Accounts" folder, but since only read and write permissions were granted, the file name remained unchanged, and no other modifications were allowed.



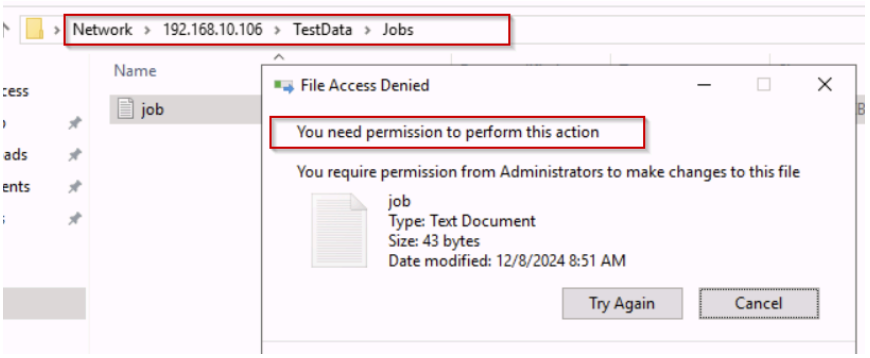
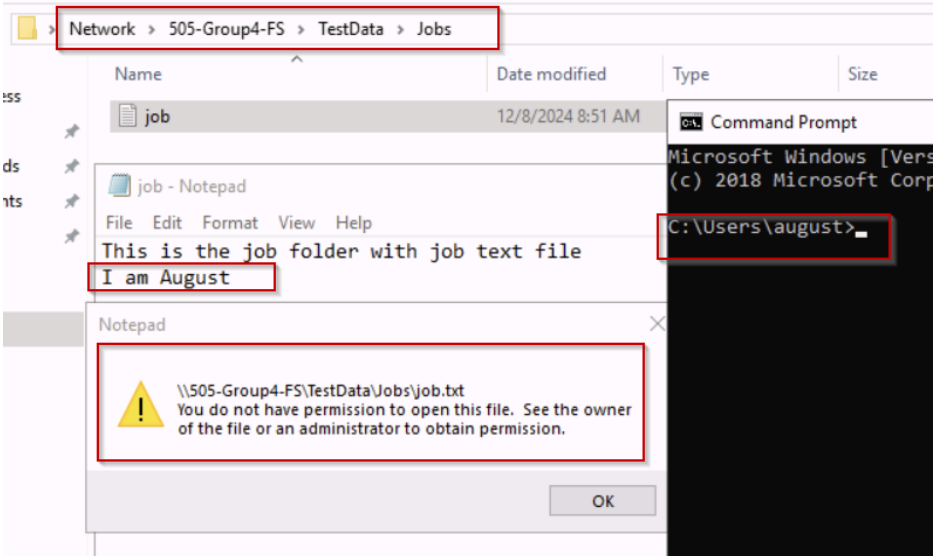


Figure 44: Testing Test2 user access

- **Testing August to read Jobs**

  The figure below illustrates that the user August has read-only access to the Jobs folder, with no permissions to modify, delete, or perform any other actions. Additionally, August has no access to make any changes in the Accounts folder.



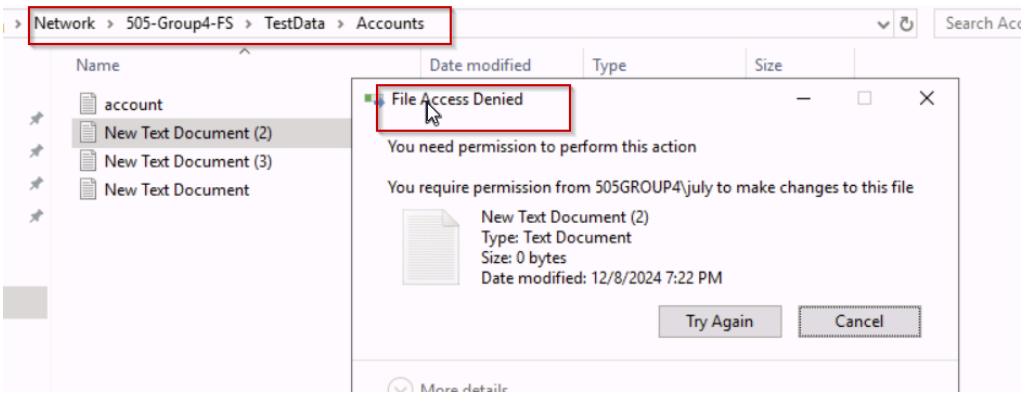


Figure 45: Testing August user access

4.2. Modify Permissions for a Specific User

To better understand role-based access control, user August has been granted “modify” permissions for the Account folder, in addition to the read-only access to the Job folder

- Giving August modify permission to the Account folder in the file server.

  We followed the same steps as before to grant user 'August' modify permission to the 'Account' folder, with the permissions being set on the File Server.

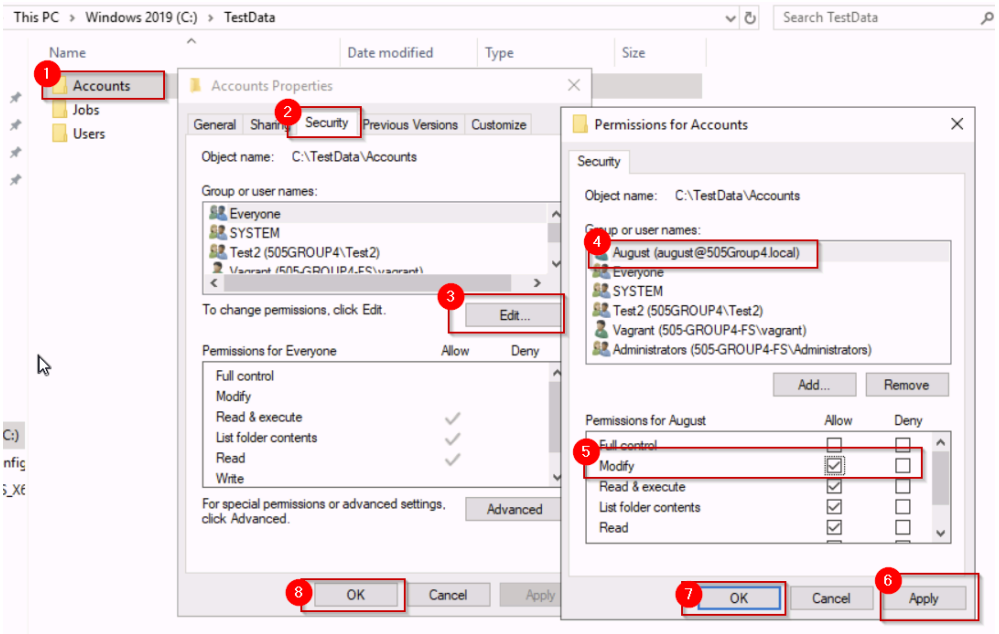


Figure 46: Modifying August user permissions

- Testing added permission on August

  The added permission should allow user August to modify the content in the "Account" folder, as demonstrated in the figure below. August user changing the default file name.

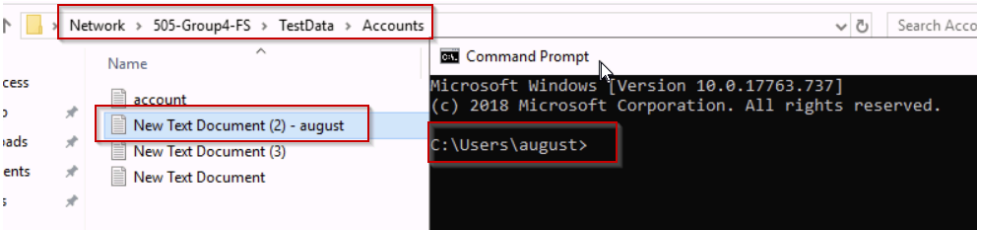


Figure 46: Testing August user permissions

4.3. Modify Group Membership

- Adding August to Test1 Group

We followed the same procedure for adding August to the Test1 group on the domain controller, as we had previously done for adding April and May to Test1. The figure below shows the step for adding August to Test1.

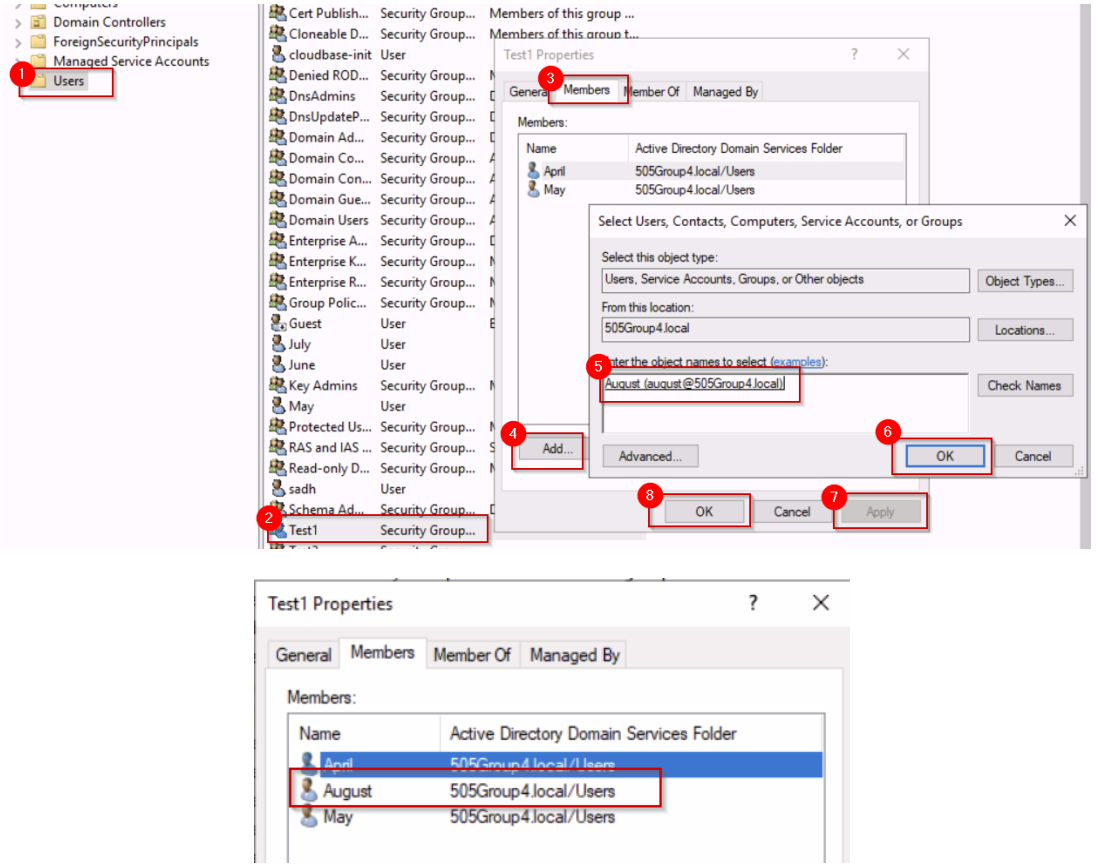


Figure 47: Modifying Group membership

- Testing the group level permission for August

After adding August to the Test1 group, the user should inherit the permissions of the Test1 group along with their own permissions. This will allow August to modify the Job folder according to Test1's permissions, while still having read-only access. August will also be able to modify the Accounts folder based on the permissions set earlier. The figure below will verify the permission sets:

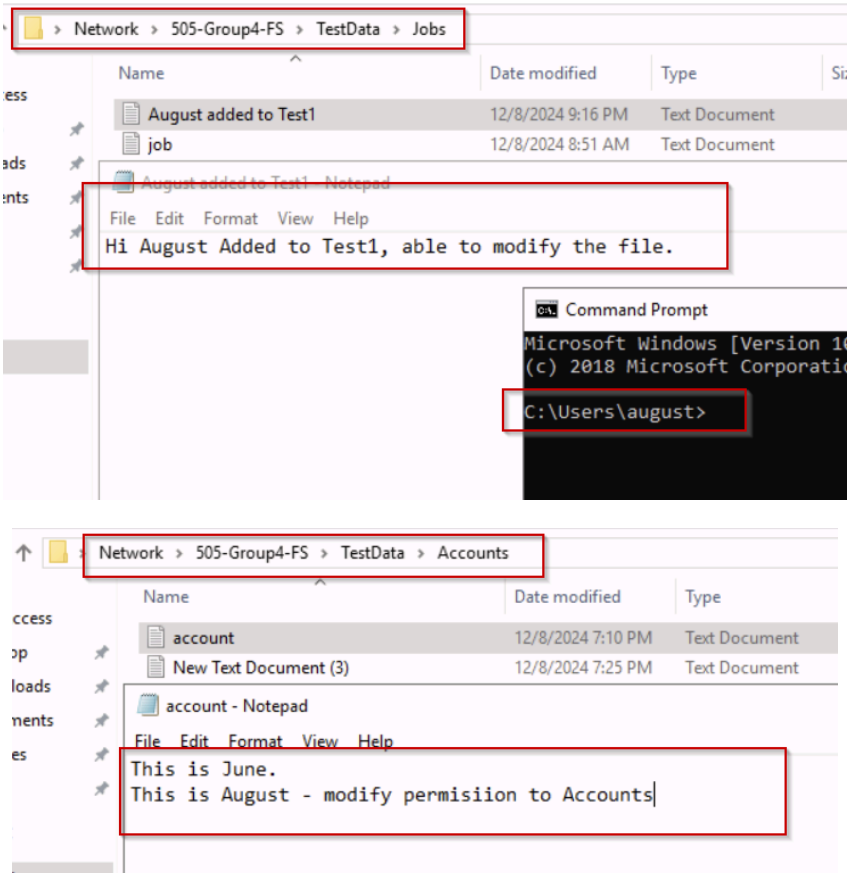


Figure 48: Testing modified group permissions

5. Hardening and Security Tools Evaluation

5.1. Tools Used

- Microsoft Hardening configuration guidelines
- PingCastle
- CIS Benchmark

5.2. Hardening the Environment

5.2.1 Microsoft Hardening configuration guidelines

Few of the Microsoft suggest hardening configuration rules were followed to harden the domain control which are described below.

5.2.1.1 Enabling Windows Defender

Windows defender is a built-in antivirus solution in Windows operating systems that integrates with Windows security centre. Enabling windows defender improves endpoint security and Active Directory relies on secure endpoints. Defender is part of Microsoft's recommended hardening guidelines, which Ping Castle uses to assess security posture.

Enabling Windows Defender demonstrates compliance with **Microsoft's baseline security** recommendations therefore ensuring compliance.

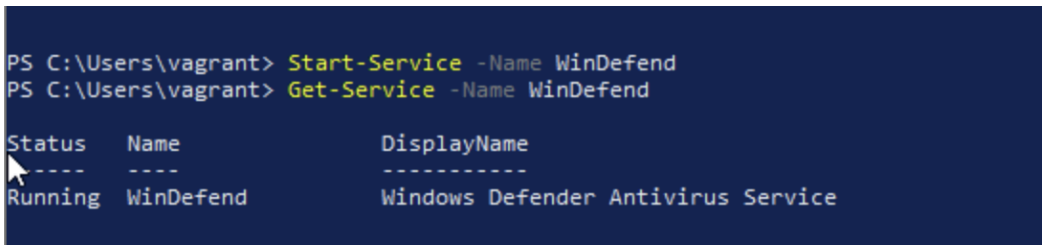


Figure 49: Stating WinDefend Antivirus Service

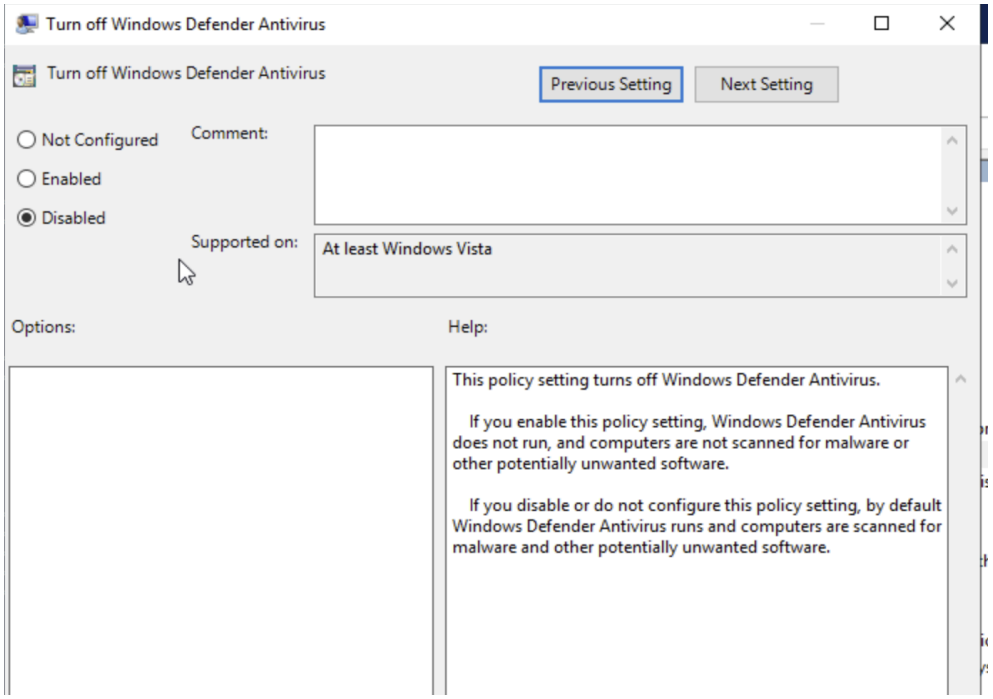
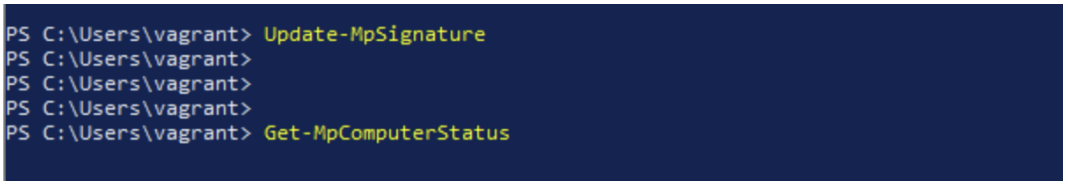


Figure 50: Disabling auto turnoff of WinDefend



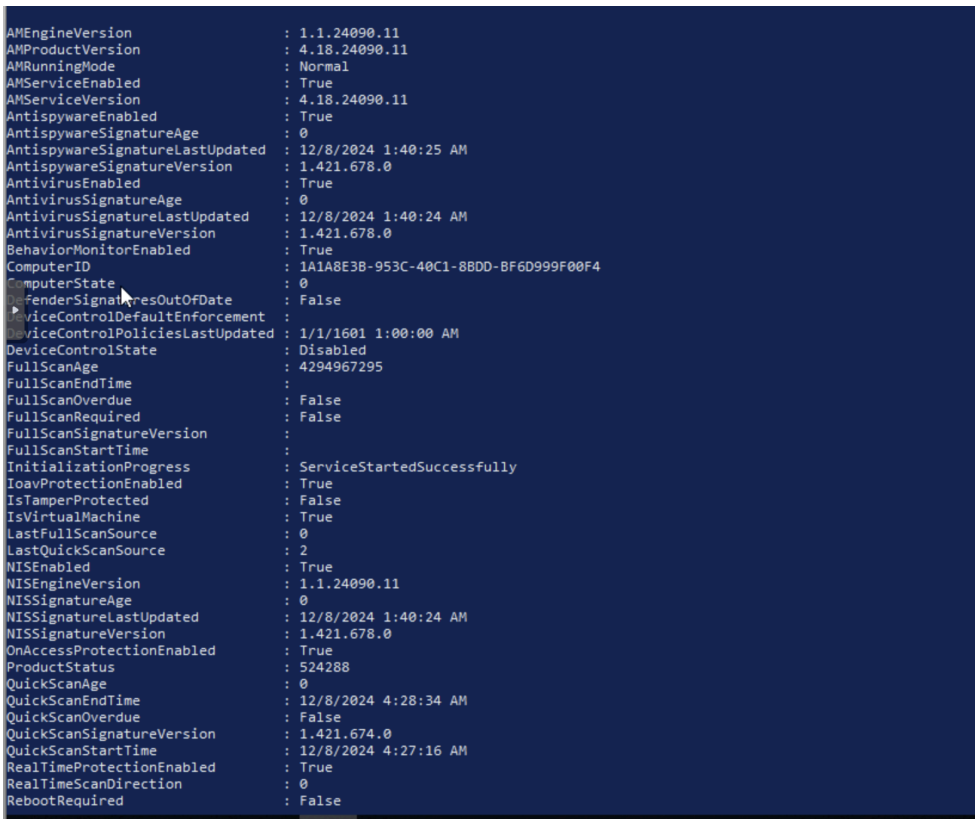


Figure 51:Getting Mp status

5.2.1.2 Enabling Recycle Bin

Using the Active Directory Recycle Bin, administrators can restore deleted AD objects (users, groups, etc.) without having to restart domain services or a backup. It preserves all linked attributes of the objects, making restoration seamless. It corresponds with Microsoft's recommendations for AD hardening and recovery planning. Enabling the AD recycle Bin strengthens the resilience and security of Active Directory.

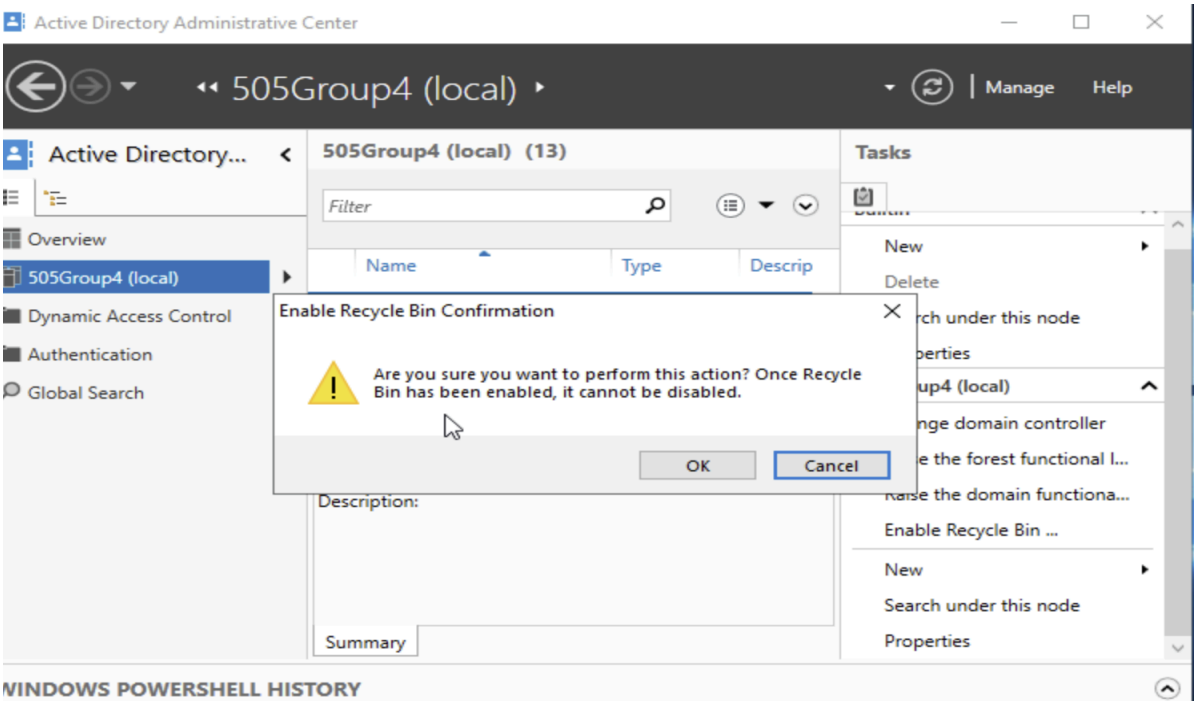


Figure 52: Enabling Recycle Bin

5.2.2 PingCastle Recommendations

Pingcastle was used to check the security of the domain controller based on which some of the steps were applied to harden the domain controller to secure it further.

5.2.2.1 Refusing LM and NTLM usage

NTLM is an outdated protocol that is susceptible to cryptographic attacks. It is often exploited by attackers who intercept network traffic to capture NTLM hashes, which can then be used to impersonate legitimate users. By default, NTLMv1 is accepted by the domain controllers. Refusing them in the LAN manager prevents exploitation of outdated protocols, reducing overall AD vulnerabilities as suggested by Pingcastle. This significantly enhances

the security and integrity of the Active Directory.

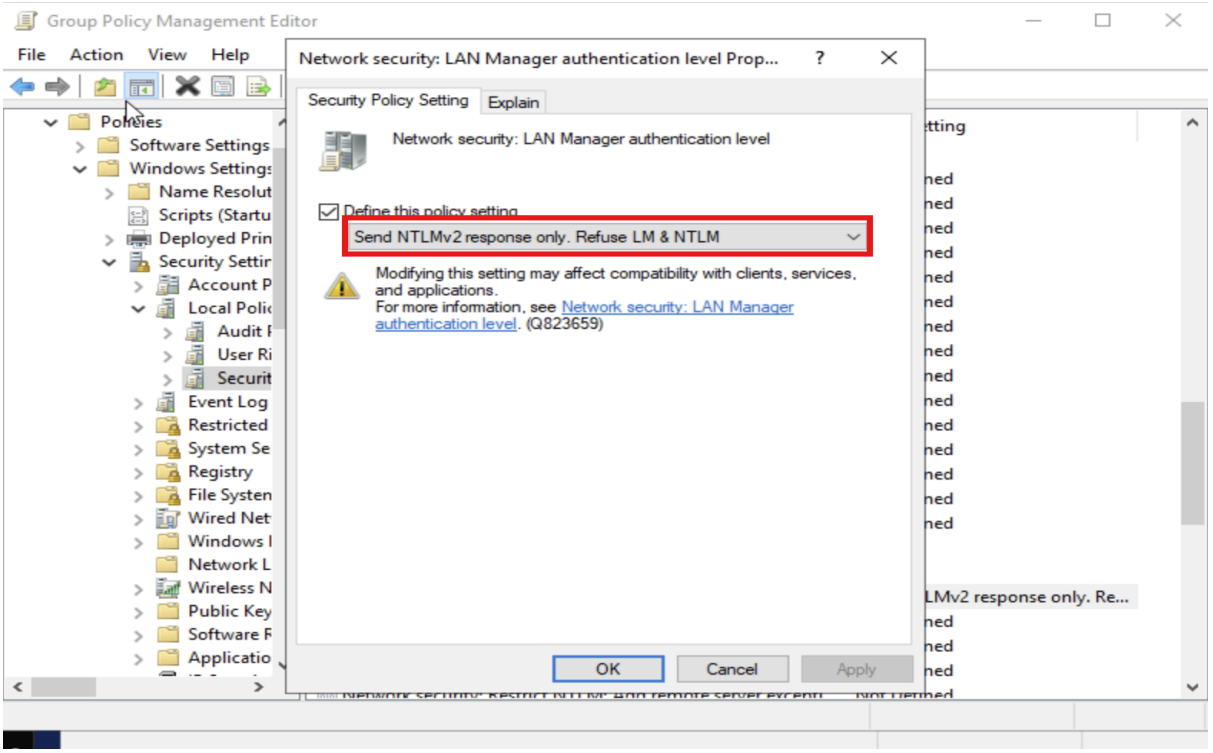


Figure 53: Refusing LM & NTLM usage in GPO

5.2.2.2 Disabling SMBv1

SMBv1 is an outdated protocol with critical vulnerabilities, making it a frequent target for cyberattacks such as ransomware campaigns. Attackers exploit SMBv1 to intercept and manipulate network traffic, gaining unauthorized access or propagating malware across the network. Disabling SMBv1 reduces the risk of such attacks and improves the overall security posture of Active Directory.

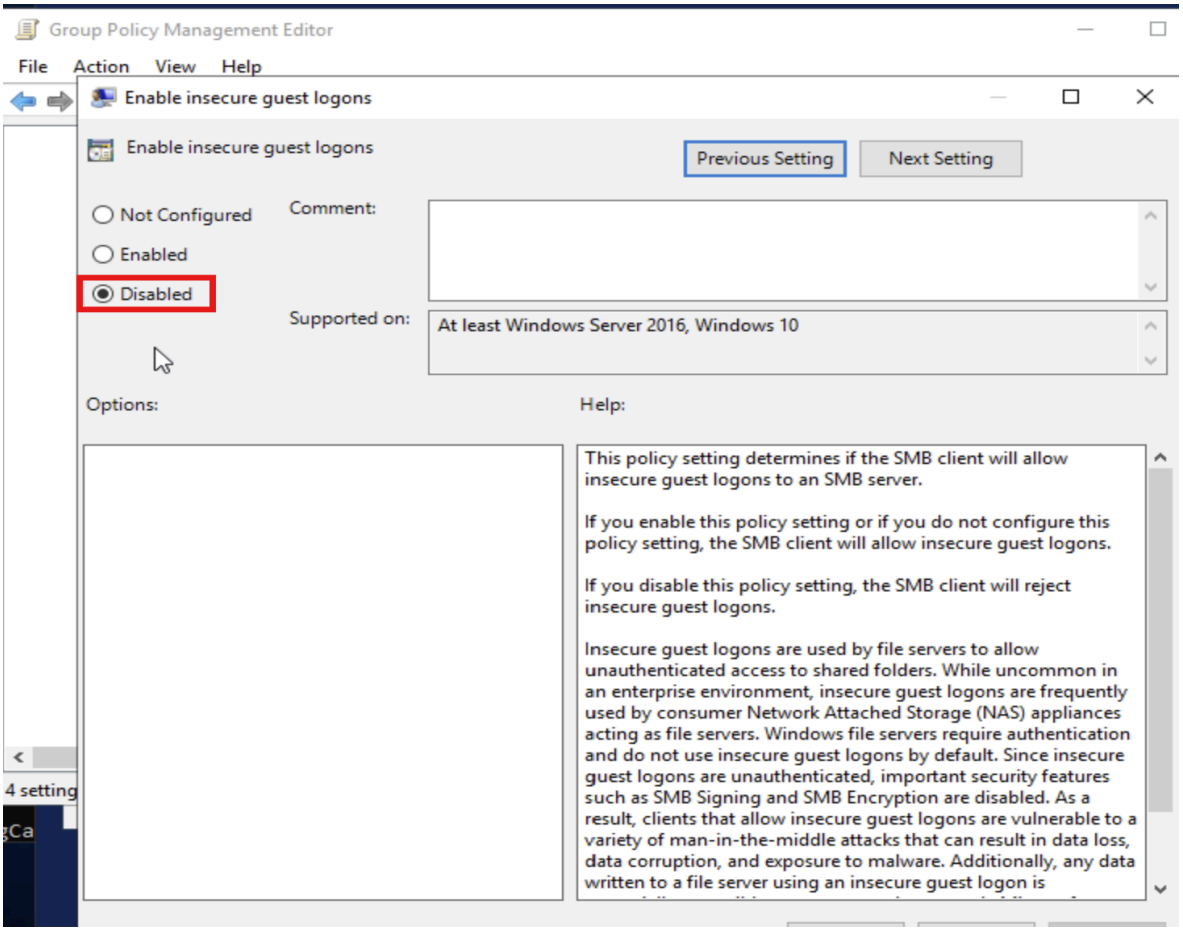


Figure 54: Disabling SMB to allow insecure guest logons

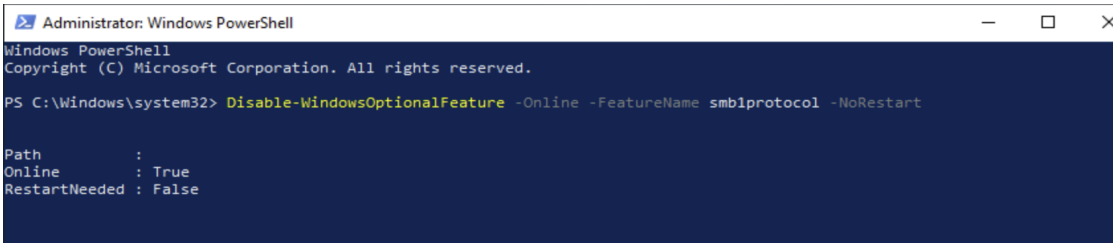


Figure 55: Disabling smb1 protocol in powershell

5.2.2.3 Remove users from Schema admins

Schema admin is a highly privileged group and the users belonging to the schema admin group can alter the schema, such as extending or modifying object definitions and it cannot be undone. It can cause significant and irreversible changes to the directory. As the Pingcastle suggests, limiting membership in this group is essential for mitigating the risk of privilege escalation and ensuring the security of the AD environment. By maintaining strict control over Schema Admins, organizations align with best practices and strengthen their security posture.

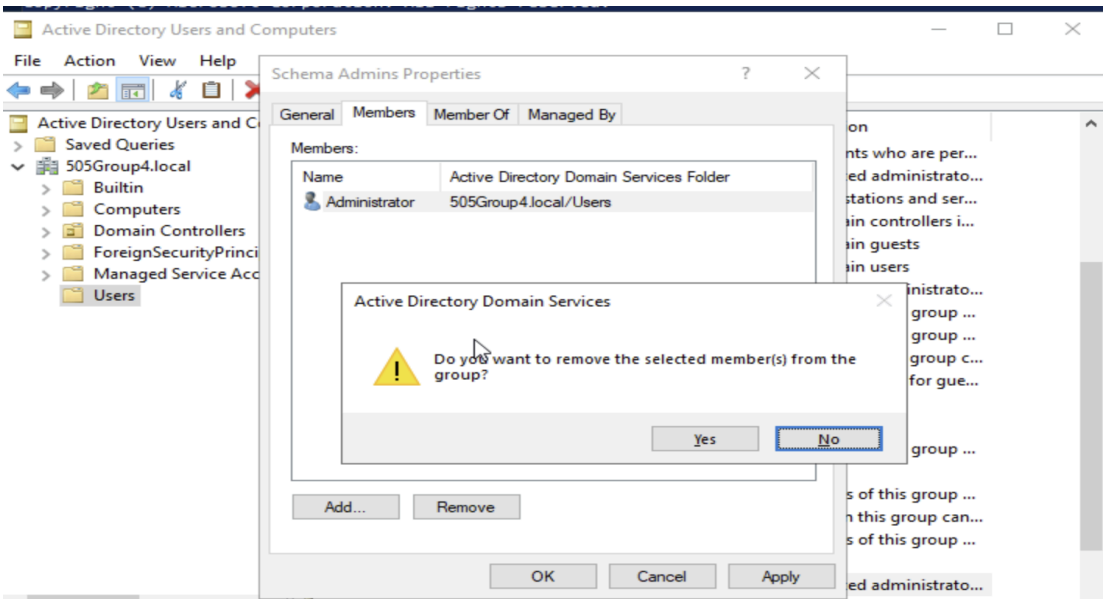


Figure 56: Emptying the schema admin group

5.2.3 CIS Benchmarks:

Few of the CIS Benchmark rules were followed to harden the domain control which are described below.

Password policies are configured in the Group policy Management editor to adhere to the CIS Benchmarks.

5.2.3.1 Password policy - Maximum password age

Password expiration duration is changed from 42 to 60 days as suggested by the CIS benchmarks.

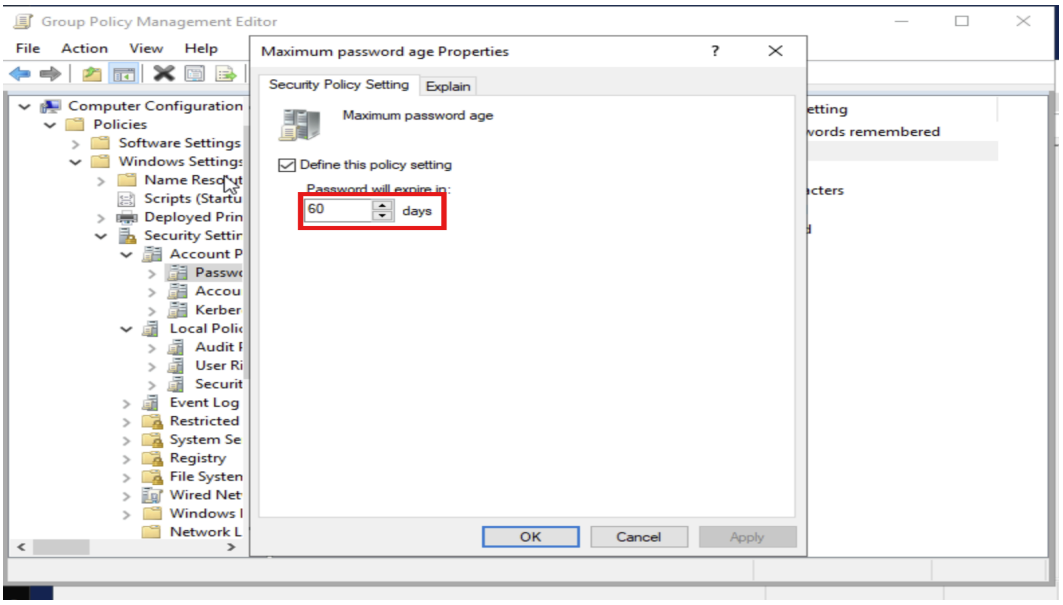


Figure 57: Password Policy setting - Maximum password age

5.2.3.2 Password policy - Minimum password length

Minimum required length for a password is changed from 7 to 14 as recommended by the CIS Benchmark.

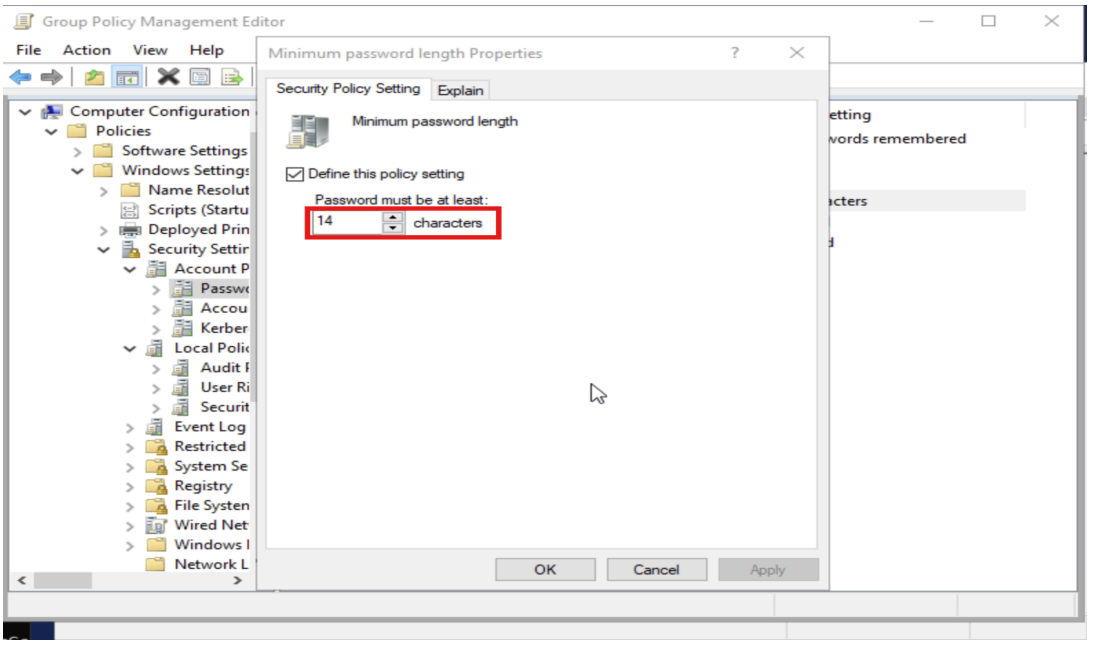


Figure 58: Password Policy setting - Minimum password length

5.3 Impact of Hardening

Before Hardening

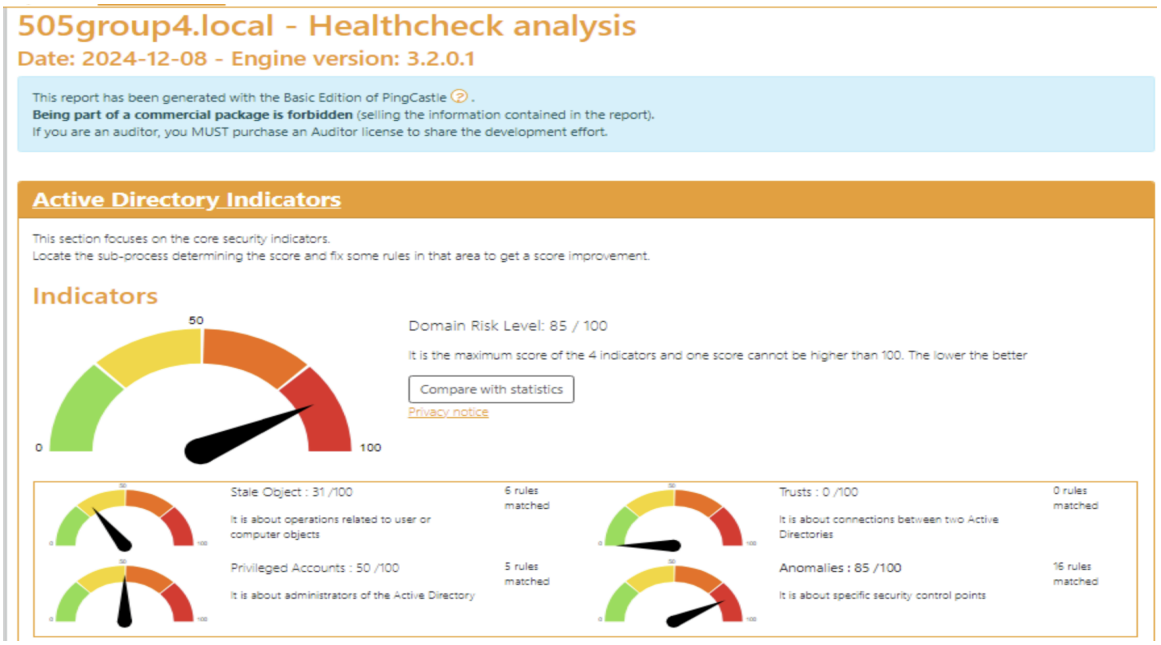


Figure 59: PingCastle score before hardening

After Hardening

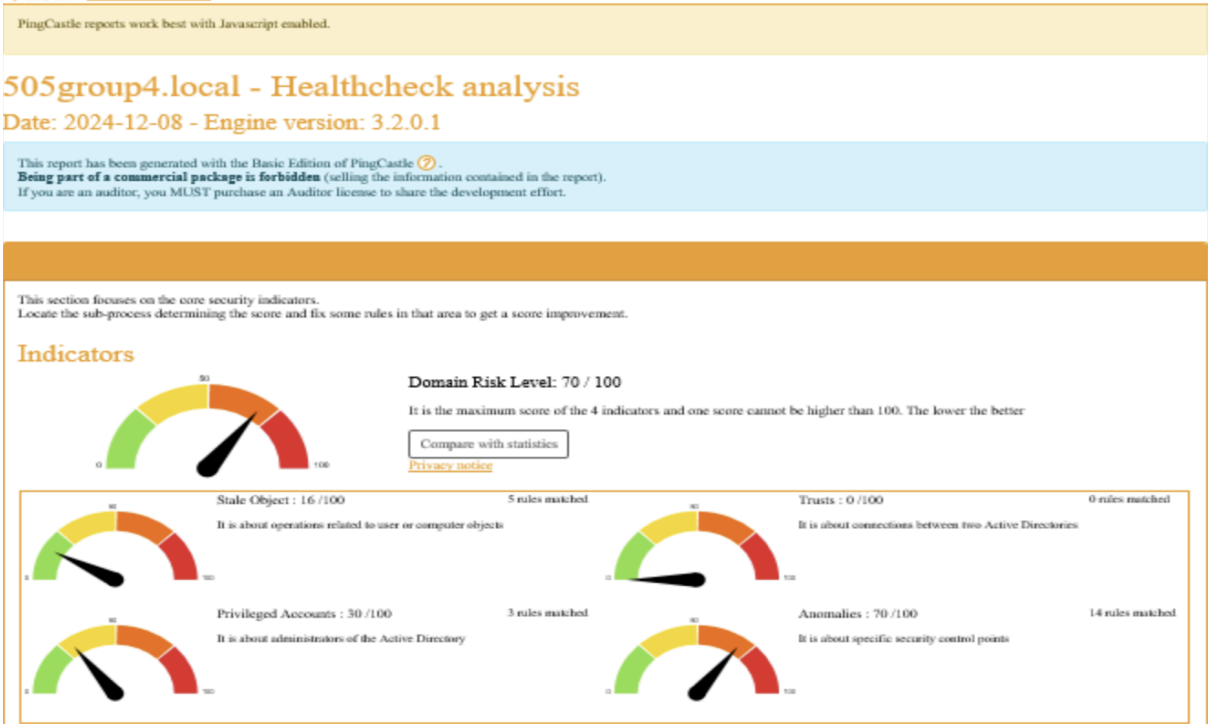


Figure 60: PingCastle score after hardening

5.3.1 Key Improvements

Stale Object:

Before Hardening: 31/100 (6 rules matched)

After Hardening: 16/100 (5 rules matched)

Impact: By cleaning up outdated or unused objects in the directory, such as old user accounts and computer objects, the score was reduced. This enhances directory hygiene and reduces potential attack vectors.

Privileged Accounts:

- Before Hardening: 50/100 (5 rules matched)
- After Hardening: 30/100 (3 rules matched)
- Impact: Restricting excessive privileges, removing unused privileged accounts, and enforcing the principle of least privilege significantly improved security for high-risk accounts.

Trusts:

- Before Hardening: 0/100 (0 rules matched)
- After Hardening: 0/100 (0 rules matched)
- Impact: Trust configurations between Active Directories were already secure and maintained with no additional issues.

Anomalies:

- Before Hardening: 85/100 (16 rules matched)
- After Hardening: 70/100 (14 rules matched)
- Impact: Addressing misconfigurations and tightening security settings reduced the number of anomalies. This strengthens the directory against potential exploitation of misaligned configurations.

Overall Domain Risk Level:

- Before Hardening: 85/100
- After Hardening: 70/100

The report indicates that, through implementing hardening techniques such as account cleanup, privilege management, and configuration corrections, the AD environment has become more resilient against threats. The improved scores across various indicators reflect the effectiveness of these actions in enhancing the overall security posture. The remaining gaps can be addressed by focussing on continuous monitoring and efforts to implement the recommendations provided by the PingCastle.

6. Challenges

Some of the challenges that we faced during this projects are:

- Replication delays or incorrectly configured linkages to Organizational Units (OUs) occasionally prevented Group Policies (GPOs) from propagating as intended. By examining GPO settings and manually refreshing policies with gpupdate /force, the problem was resolved.
- It was necessary to precisely configure administrator credentials and domain connection in order to join the File Server to the domain. Network problems caused this process to be delayed.

- Enforcing password complexity requirements and turning down SMBv1 while preserving system usability proved to be difficult to implement. Prioritized vulnerabilities and identified them using tools like PingCastle and CIS Benchmarks.

7. Lesson Learned

- Understanding the interdependencies between DNS, DHCP, and file servers inside the domain environment was crucial to the successful integration of these components.
- Using groups for RBAC decreased administrative burden and made permission assignments easier and effective.
- By using tools like PingCastle and following CIS Benchmarks, the team was able to gradually harden the environment by gaining important insights into potential vulnerabilities and misconfigurations.
- Limitation and advantage of role based access control

8. Conclusion

As a result, a safe and functional Active Directory that is connected to necessary infrastructure services was established. A deep understanding of Active Directory configuration and administration by setting up a Windows Server 2019 Domain Controller, File Server, and client PCs are demonstrated. Effective domain management and operational dependability were guaranteed by the smooth integration of Active Directory Domain Services (AD DS) with crucial infrastructure services like DNS and DHCP. Group Policies (GPOs) and Role-Based Access Control (RBAC) were used to make sure that groups and users were arranged efficiently and that permissions were allocated safely.

The initiative also stressed how crucial it is to use security best practices, such enforcing strict password regulations, turning off outdated protocols, and following CIS Benchmarks, in order to harden the environment. Finding vulnerabilities and verifying setups were made possible by tools like PingCastle. Through methodical debugging and cautious planning, issues including GPO misalignment, file server integration, and tool compatibility were successfully resolved.

Important takeaways were the importance of comprehensive documentation, the necessity of testing policies and permissions, and how to strike a balance between security and usability in a real-world setting. These encounters gave us important knowledge on how to implement and protect enterprise-level directory services.

9. References

Best Practices for Securing Active Directory. (n.d.). Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

CIS Microsoft Windows Server Benchmarks. (n.d.). CIS Center for Internet Security. Retrieved December 8, 2024, from https://www.cisecurity.org/benchmark/microsoft_windows_server

David F. Ferraiolo and D. Richard Kuhn. (n.d.). *Role based access control*, 554-563. https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased-access-controls/final/docs/ferraiolo-kuhn-92.pdf

What Is a Domain Controller? - IT Glossary. (n.d.). SolarWinds. Retrieved December, 2024, from https://www.solarwinds.com/resources/it-glossary/domain-controller

Wright, G. (n.d.). *What is a file server and how does it work?* TechTarget. Retrieved December, 2024, from https://www.techtarget.com/searchnetworking/definition/file-server